An Approach to Assessment of Reliability of Passive Safety Systems

Sergey Galushin[a*], Graeme Trundle[b], Manorma Kumar[c], Anders Olsson[d]
[a] Vysus Group, Solna, Sweden , sergey.galushin@vysusgroup.com
[b] Royal Institute of Technology, Stockholm, Sweden, trundle@kth.se
[c] Vysus Group, Chicago, USA, manorma.kumar@vysusgroup.com
[d]Vysus Group, Malmö, Sweden, anders.olsson@vysusgroup.com

Abstract: Passive safety systems are increasingly implemented in advanced nuclear power plant designs. These systems rely on intrinsic, physics-based driving forces of low magnitude, enabling fully passive operation without active components. However, the small magnitude of these forces makes system performance more sensitive to disturbances, boundary conditions, and uncertainties in the underlying physical phenomena, thereby complicating reliability assessment compared to active systems.
This paper illustrates the application of an approach for assessing the reliability of passive safety systems, based on the Reliability Methods for Passive Systems (RMPS) methodology and Bayesian inference, to the isolation condenser system (ICS) of the BWRX-300 small modular reactor (SMR).
Application of the approach yielded an extremely low estimated probability of failure for the natural circulation in the isolation condenser system. To account for residual uncertainty, a conservative failure probability of 1.E-7 was assigned based on engineering judgment. The results were subsequently incorporated into a simplified PSA model of the BWRX-300 to evaluate system-level unavailability and the overall Core Damage Frequency (CDF).

1. INTRODUCTION

Passive safety systems are being given an increasingly large role in the design of future nuclear power plants (NPP). Such systems utilize natural phenomena in their operation, in contrast to active systems, which may require an external power source. As a result, they generally offer greater reliability and simplicity at a much-reduced cost, leading to their widespread adoption. Nonetheless, passive safety systems pose a unique challenge for the assessment of NPP safety. While their reliability is generally regarded as superior to their active counterparts, the quantification of this reliability has no clear-cut methodology. Systems which rely on active components may draw from a large body of reliability data, for which no passive analog exists. Further, while the forces passive systems rely on may be omnipresent (e.g., gravity), the magnitude of those forces may be contingent on other phenomena which are either poorly understood or difficult to quantify.
According to IAEA-TECDOC-1752 [5] a passive component is one that performs its intended function without the need for external power sources, control signals, or operator actions. Passive components are classified into four categories based on their level of passivity and internal complexity [5]:

- **Category A**
  This category is characterized by:
  - no signal inputs of "intelligence", no external power sources or forces,
  - no moving mechanical parts,
  - no moving working fluid.
- **Category B**
  This category is characterized by:
  - no signal inputs of "intelligence", no external power sources or forces,
  - no moving mechanical parts, but
  - moving working fluids.
    The fluid movement is only due to thermal-hydraulic conditions occurring when the safety function is activated.

- **Category C**
  This category is characterized by:
  - no signal inputs of "intelligence", no external power sources or forces; but
  - moving mechanical parts, whether or not moving working fluids are also present. The fluid motion is characterized as in category B; mechanical movements are due to imbalances within the system (e.g., static pressure in check and relief valves, hydrostatic pressure in accumulators) and forces directly exerted by the process.
- **Category D**
  This category addresses the intermediary zone between active and passive where the execution of the safety function is made through passive methods as described in the previous categories except that internal intelligence is not available to initiate the process.

Category A passive features are typically design provisions whose functions are to eliminate initiating events of certain accidents, prevent the propagation of such events into design basis accidents (DBAs), or inhibit the escalation of DBAs into severe accidents involving significant radioactive releases. Their reliability is generally ensured through the application of sound engineering principles, compliance with applicable codes and standards, and the implementation of robust quality assurance and in-service inspection programs.

In contrast, Categories B, C, and D rely on physical processes such as natural circulation, pressure-driven flows, or internal mechanical responses. These systems require validation and testing to confirm reliable operation and to optimize design if necessary.

While individual processes (e.g., fluid expansion, pressure drop) may be well understood, their combined behavior under varying boundary conditions, system states, or component malfunctions can introduce significant uncertainty. Thus, process performance reliability is a central concern in the evaluation of these systems.

Phenomena such as natural circulation may exhibit higher intrinsic reliability than active components. However, the reliability assessment of active systems benefits from a large body of operational data and standardized methods. In contrast, the reliability evaluation of passive systems is inherently design-specific and, at present, lacks an industry-wide standard for methodology. Furthermore, the driving forces behind natural circulation, such as temperature gradients, density differences, and system geometry, are dependent on several interrelated factors. These factors are often poorly characterized or subject to large epistemic uncertainties, which complicates reliability assessment.

Properly accounting for uncertainty in passive safety systems and understanding its implications for the overall safety analysis of plants that depend on them, remains an unresolved challenge. In particular, three major open issues have been identified in the reliability assessment of passive systems [3]:

- Uncertainties
  Passive system reliability is difficult to quantify due to the uncertainties in the thermal-hydraulic (T-H) phenomena that drive these systems.
- Dependencies
  Many critical parameters, those with significant influence on the natural driving forces, may not be statistically independent. Treating them as independent in probabilistic models can lead to an overestimation of system reliability. Properly capturing these dependencies is essential to avoid biased results.
- Integration
  Passive systems often exhibit behavior that does not conform neatly to binary “success/failure” logic. Instead, they may operate in intermediate or degraded states that depend on nuanced physical conditions. This complexity complicates their integration into traditional probabilistic safety assessments (e.g., event tree/fault tree models), where assumptions of discrete system states may not fully capture reality.

Therefore, addressing the aforementioned issues in assessing passive system reliability generally involves these critical parameters. This may be done by either analyzing the components which affect these critical parameters, or by analyzing how deviations in these parameters affect system operation.

2. METHODOLOGY

The most established framework for such analysis is the Reliability Methods for Passive Systems (RMPS) methodology [4]. RMPS quantifies the failure probability of a passive safety system by propagating uncertainties in critical parameters through a validated T-H model.
The RMPS methodology addresses the following issues:

- Identification and quantification of the sources of uncertainties and determination of the important variables;
- Propagation of the uncertainties through T-H system models and assessment of passive system unreliability;
- Integration of the calculated unreliability into PSA accident sequence analyses.

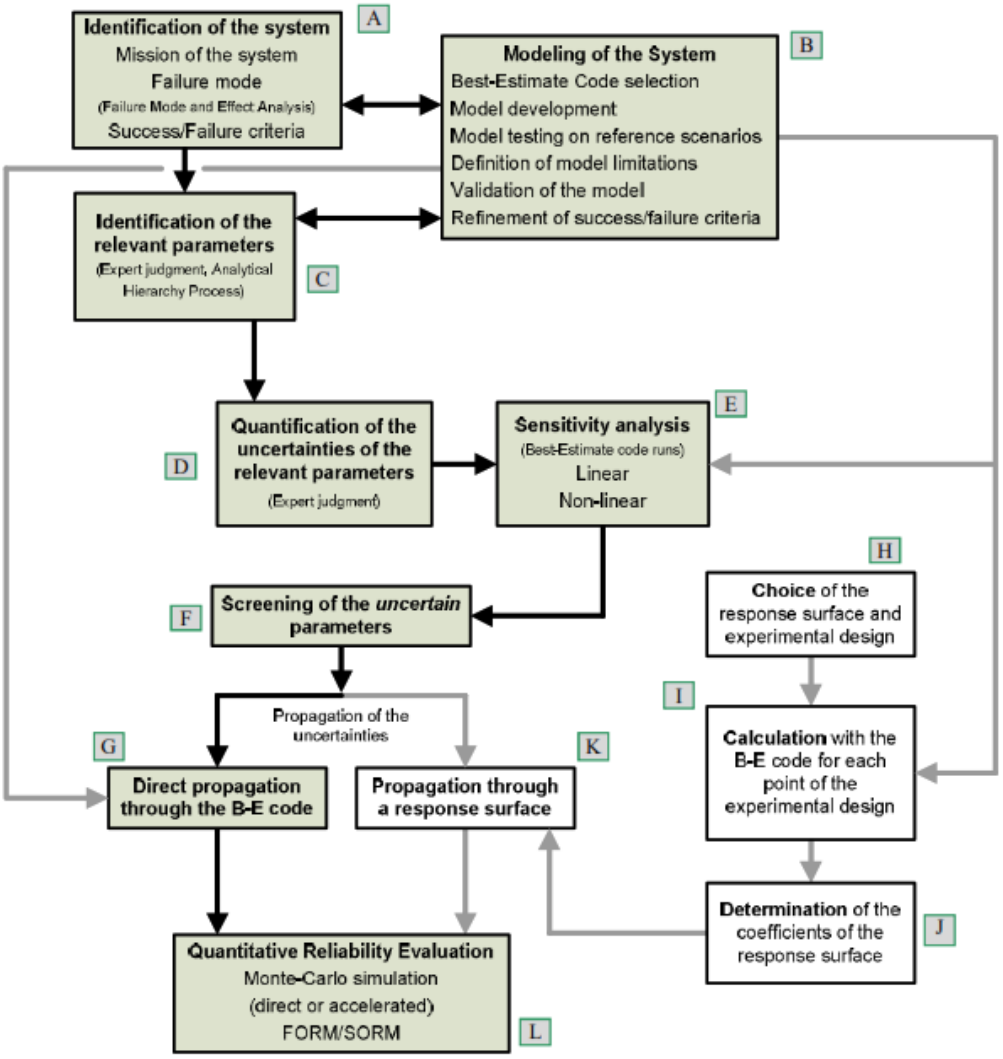

Figure 1. RMPS methodology flowchart [5].

The proposed methodology consists of several steps, which are shown in Figure 1 and are detailed below.

2.1. Analysis steps in RMPS methodology

The description of the analysis steps in the RMPS methodology is based on [5].

Accident scenario definition

The RMPS methodology begins with defining the accident scenario in which the passive safety system is expected to operate. Scenario definition enables identification of relevant failure criteria, critical parameters, and uncertainty sources. Because passive system behavior depends strongly on boundary conditions and transient evolution, reliability results are scenario specific. Overall system reliability is obtained by integrating scenario-level unreliability into the plant Probabilistic Safety Assessment

(PSA). Unlike conservative approaches based on worst-case assumptions, RMPS evaluates system performance across a representative uncertainty space, which is more appropriate for passive systems characterized by nonlinear thermal-hydraulic interactions and non-monotonic responses.

System characterization

The system is characterized by defining its functional role, mission time, potential failure modes, and success/failure criteria. The functional role describes the intended safety function, such as decay heat removal, reactor vessel cooling, or primary system depressurization. Failure modes are identified using qualitative techniques such as Failure Modes and Effects Analysis (FMEA), accounting for complex thermal-hydraulic phenomena and system interactions. In some cases, "virtual" components representing key physical processes (e.g., natural circulation) are introduced. Success and failure criteria are typically defined as threshold values of relevant physical variables (e.g., temperature, pressure, or flow rate) within the mission time.

System modeling and identification of uncertainties

Due to limited experimental data under realistic conditions, passive system performance is mainly evaluated using best-estimate thermal-hydraulic simulations. A reference model with nominal parameter values is developed and validated against available experimental data where possible. Modeling may reveal additional failure mechanisms, such as flow oscillations or non-condensable gas accumulation, which must be incorporated into the reliability assessment.

Uncertainty sources generally fall into two categories:

- Modeling uncertainties (epistemic), arising from simplified physical models, empirical correlations, or geometric approximations;
- Input parameter uncertainties (aleatory), including initial and boundary conditions, material properties, and other relevant parameters.

These uncertainties are identified using available data and expert judgment.

Uncertainty characterization

Probability distributions are assigned to uncertain parameters to represent the current state of knowledge. When sufficient data exist, statistical methods can be used to estimate distributions; otherwise, expert judgment is required. In the absence of strong evidence, uniform distributions are often adopted to represent epistemic uncertainty. Dependencies between parameters must also be considered, since assuming independence may distort failure probability estimates

Sensitivity analysis

Because thermal-hydraulic models may contain numerous uncertain parameters, sensitivity analysis is used to identify the dominant contributors to variability in key figures of merit. This allows the analysis to focus on parameters that most strongly influence system performance and reliability, improving computational efficiency and the robustness of the reliability assessment. An overview of applicable sensitivity analysis methods can be found in [1].

Reliability evaluation

Different methods can be employed to quantify the reliability (or conversely, the failure probability) of a passive system.

Passive system reliability can be quantified using several approaches based on a failure function comparing a key figure of merit (FOM) with its threshold:

$$M = FOM - FOM_{Goal} = g(x_1, x_2, \dots, x_n) \quad (1)$$

where x_i $(i = 1, \dots, n)$ are the n basic random variables (input parameters), and $g(x_1, x_2, \dots, x_n)$ is the functional relationship between the random variables and the failure of the system. The failure function can be defined in such a way that the limit state, or failure surface, is given by $M = 0$. The failure event is defined as the space where $M \leq 0$, and the success event is defined as the space where $M > 0$. Thus, the probability of failure can be evaluated by the following integral:

$$P_f = \iint \dots \int f_x(x_1, x_2, \dots, x_n) dx_1 dx_2 \dots dx_n \quad (2)$$

where f_x is the joint probability density of the input variables. Since this integral is generally intractable due to nonlinear interactions between variables, numerical methods are used.

IAEA TECDOC-1752 [5] propose the following methods for quantification of P_f:

- **Monte Carlo simulation.**
  Direct Monte Carlo sampling estimates the failure probability by repeatedly sampling input parameters from their distributions and evaluating the failure function. The fraction of samples with $M \leq 0$ gives Pf. Efficiency can be improved using variance reduction techniques such as importance sampling or stratified sampling, which are particularly useful for estimating small failure probabilities.
- **First- and Second-Order Reliability Methods (FORM/SORM).**
  FORM/SORM approximate the failure probability by transforming input variables into a standard normal space, identifying the design point (minimum distance to the limit state), and locally approximating the failure surface. These methods are computationally efficient for small failure probabilities but rely on smooth limit-state functions and local approximations, making accuracy difficult to assess.
- **Surrogate models.**
  To reduce computational cost when high-fidelity simulations are required, surrogate (response surface) models can approximate system behavior. Common approaches include, e.g., polynomial regression, artificial neural networks, generalized linear models. These models are trained on a limited set of simulations and then used to rapidly evaluate the failure function, with the surrogate approximation error considered in the reliability estimate.

Bayesian estimation

In addition to the methods described above, Bayesian approaches can be used to estimate the failure. In addition to the methods described above, Bayesian approaches can be used to estimate the failure probability of passive systems by constructing probabilistic models for the figure of merit (FOM) predicted by a T-H code under uncertainty. Bayesian inference provides a structured framework for combining simulation results with prior knowledge and expert judgment.

In this framework, the FOM is assumed to follow a parametric probability distribution (e.g., normal or lognormal) whose parameters are not known a priori. These parameters are assigned prior distributions based on expert judgment, physical reasoning, or previous studies. Simulation results obtained from T-H code runs under uncertainty propagation of input parameters are then used to update the prior distributions via Bayes' theorem, yielding posterior distributions of the FOM parameters.

From the posterior distributions, a posterior predictive distribution for the FOM is constructed. This distribution represents the expected variability in system performance, accounting for both observed variability and uncertainty in the model parameters. The failure probability is subsequently estimated as the probability that the FOM exceeds a defined safety threshold.

This method is particularly advantageous when the number of T-H simulations is limited, prior knowledge about expected FOM behavior is available, or quantification of uncertainty in the estimated failure probability is required. For these reasons, the Bayesian approach described above is employed in the present study.

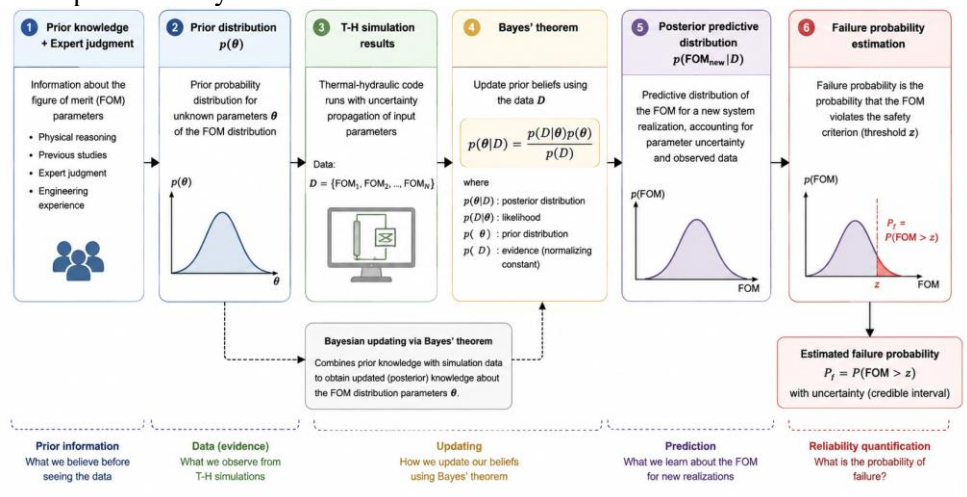

Figure 2. Bayesian approach to quantification of the failure probability

Integration of Passive System Reliability in PSA

The integration of passive system reliability into PSA is most commonly achieved by incorporating passive systems into the event tree (ET) structure used to represent accident sequences. In this representation, each branch of the event tree corresponds to a unique combination of successes and failures of safety systems in response to a specific initiating event.

In Level 1 PSA, the consequences of each sequence are typically expressed in terms of the degree of reactor core damage. These consequences are usually evaluated using T-H calculations, often performed in a conservative manner.

While event tree modeling is conceptually simple and widely used, it may seem insufficient to represent the dynamic behavior of passive systems, which often involve time-dependent interactions, feedback mechanisms, and system-initiated responses. However, in practice, these dynamic system interactions can be accounted for by embedding detailed T-H modeling into the reliability assessment. This approach allows passive system behavior to be evaluated realistically, even within a traditionally static ET framework.

For accident sequences where no clear bounding (or "envelope") case can be defined, an additional event is introduced into the event tree to explicitly represent failure of the physical process (e.g., failure of natural circulation). In these cases, uncertainty analyses are performed to evaluate the corresponding failure probabilities. These probabilities are then incorporated into the appropriate event tree branches.

In practical PSA implementations, the passive system can be represented within a fault tree (FT) structure, which is then embedded as a function event within the overarching event tree. This FT can include both passive and active components and may be conditioned using house events and boundary conditions to reflect different accident sequences. This enables the modeling logic to select appropriate basic events that represent the passive system's behavior under varying process parameters, system requirements, and success criteria.

Other Considerations

One primary limitation of RMPS is the modeling uncertainty and user effect, as the fidelity of the T-H model plays a critical role in the accuracy of the results. The selection of nodalization schemes, modeling assumptions and user expertise can introduce variability that affects the final reliability estimate. As a result, many parameter uncertainties must be derived from expert judgment, which introduces subjectivity into the process.

Another important aspect is the computational cost. When estimating small failure probabilities (e.g., on the order of 1.0E-6), direct Monte Carlo simulation may require a prohibitively large number of simulations to achieve statistically meaningful results. For systems with complex dynamics and long simulation times, the use of surrogate models (SMs) or Bayesian techniques is essential to reduce simulation time while preserving prediction accuracy.

Lastly, due to scenario-specific nature of the RMPS methodology, the analysis must be performed independently for each transient scenario or initiating event.

3. ICS RELIABILITY ASSESSMENT

To demonstrate the approach to reliability assessment of the passive safety system the reliability assessment of the Isolation Condenser System (ICS) of the BWRX-300 was performed.

Using FMEA, critical component failure modes of the ICS were identified, including common cause failures, system dependencies, and integration of the assessment performed regarding the reliability of natural circulation as motive force for system operation. These failure modes were then incorporated into fault trees to calculate the reliability of the system as a whole, quantified by system unavailability.

In keeping with the claim that the ICS design is passive and to limit the scope of the analysis, only passive and automated system features were considered. Further, system operation was only considered over a 24-hour mission time, in-line with the ESBWR PRA [6]; this additionally precludes any consideration that failed system components are repaired over this period. Further, no spatial events were considered in the analysis.

Thermal-hydraulic studies of parallel operating loops, natural circulation stability and effects of non-condensable gases are outside of the scope of this study.

3.1. System function

The Isolation Condenser System provides decay heat removal upon the anticipated loss of the normal heat sink or isolation of the RPV, as well as over-pressure protection for the RPV. This is accomplished by the successful operation of at least one of three ICS loops .

3.2. System description and operation

The system consists of three identical loops, each consisting of:

- a pair of heat exchangers (ICHX-1/2);
- an ICS pool (IC-POOL), above and outside the containment, into which the heat exchangers are submerged;
- steam supply and condensate return lines to/from the RPV, which supply both heat exchangers (IC-PIPING);
- a pair of RPV isolation valves in series, integral to the RPV, for each supply/return line (ICV-1/2 and ICV-3/4, respectively); and
- a pair of condensate return valves, in parallel (ICV-5/6).

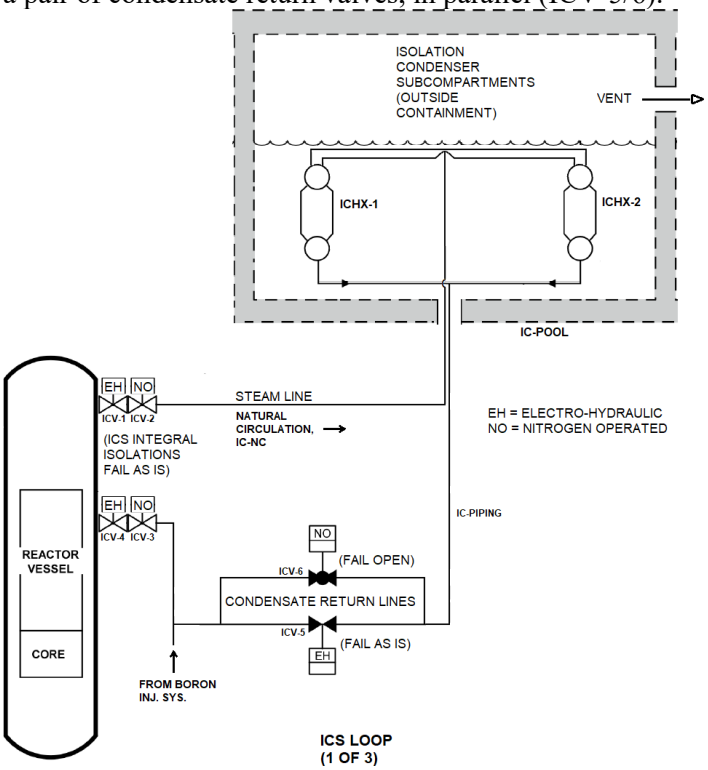

Figure 3. The BWRX-300 Isolation Condenser System, adapted from details provided in [7]

The ICS is normally at reactor pressure, as it is only isolated from the RPV by the condensate return valves. Heat transfer from the condensate return piping upstream of ICV-5 and 6 to the ICS pool will therefore cause condensate to form within the piping. System operation is commenced by opening either condensate return valve, allowing the condensate to drain into the core and establishing flow by natural circulation. Steam will be drawn from the RPV into the heat exchangers, where it will be condensed by heating and evaporating the water in the ICS pool, which vents to atmosphere.

Each loop has a rated heat transfer capacity of 33 MW [7], which is deemed sufficient for 100% emergency core cooling capacity [9]. The condensate return valves are assumed identical in design to that of the ESBWR, the operation for which are diverse: one is electro-hydraulically operated and fails-as-is (ICV-5), and the other is nitrogen-operated and fail-open (ICV-6) [6].

3.3. System dependencies

The following interfacing system dependencies are accounted for:

- Injection from the Boron Injection System (BIS) is supplied at the condensate return line of each ICS loop. It is not explicitly known how the operation of the BIS would affect the core cooling

capacity of the IC system. To simplify the analysis, it is assumed that boron injection would have no deleterious effect on ICS operation.

- Electro-hydraulically operated isolation valves ICV-1/4 and actuation valve ICV-5 are assumed to be powered by a sufficiently diverse and redundant safety-related bus. Nevertheless, loss of power to these valves may affect the isolation function in LOCA scenarios and the opening of ICV-5 during transient events. This failure mode has not been considered within the scope of the current analysis but should be included in future iterations.
- Nitrogen operated isolation valves ICV-2/3 and actuation valve ICV-6 are assumed to each be supplied by their own accumulator dedicated for their individual operation. The failure of the valve accumulator is assumed to be considered within the basic event of mechanical failure to operate.
- The isolation valves (ICV-1, 2, 3, and 4) are assumed to operate based on the actuation logic provided by the Leak Detection and Isolation system (LD&IS), which may supply three independent input signals to each valve.
- The actuation valves ICV-5 and ICV-6 are assumed to operate based on a three-channel and two-channel redundant actuation logic, respectively. This is based on the ESBWR ICS design [6].

3.4. Common Cause Failures of System Components

The common cause failure of the actuation valves (ICV-5/6), as well as the heat exchangers (ICHX-1/2), are considered in this analysis. For the actuation valves, this included all possible CCF combinations. For the heat exchangers, all possible combinations involving two units are explicitly considered. To simplify the model, all combinations involving three or more units are included within the 'CCF of All ICS HX' event (ICS-HX00-F) based on values provided in the ESBWR PRA [6], assuming that four, five, and six concurrent failures are each 10% as likely as the last and by considering the number of combinations available. This is expected to be conservative, as most combinations involving three concurrent heat exchanger failures will not directly cause system failure. Probabilities for occurrence are found in [8].

4. RESULTS

The system model used in this study is a TRACE (v5.0 patch 9) model of the BWRX-300, previously developed in [10]. The model includes a 3D vessel component, a simplified core representation with average, peripheral and hot channel groupings, and control systems to establish steady-state operating conditions. The ICS and associated boundary conditions are also explicitly modeled. The model has demonstrated good agreement with reference TRACG results and has been used to simulate a full-power reactor trip transient with isolation condenser actuation. The description of the model can be found in [10]; in the present work, the results of that study are used as input to the reliability assessment. The transient analysis of the BWRX-300 was performed iteratively, with the critical parameters sampled individually according to the distributions described in [10]. The sampling was carried out using the built-in SNAP uncertainty plug-in. A total of 93 iterations were simulated to achieve a 95% confidence level in the results, as determined using Wilks' method and computed automatically by DAKOTA [11]. The resulting distributions for the acceptance criteria parameters, PCT and pressure, are tabulated in Table 1.

Table 1. Output Distributions of Derived Acceptance Criteria

Parameter	Normal Dist. Parameters (μ, σ)	Acceptance Criteria
Peak system pressure	(7.7775 MPa, 4.30 kPa)	15.45 MPa
Peak cladding temperature	(569.40 K, 0.05 K)	1204℃.

Generally, the peak values for the acceptance criteria during the transient show less variation compared to the previous work [8][12].

4.1. Quantification of failure probability of ICS natural circulation

The probability of failure of natural circulation was quantified using the inverse cumulative distribution function and Bayesian approaches using the peak cladding temperature distribution generated by the TRACE code. In the frequentist approach, the probability of failure is estimated as the fraction of simulated scenarios in which the PCT criterion is exceeded.

As discussed in Section 2.1, in the Bayesian approach, it is assumed that the true temperature follows a probability distribution with unknown parameters. These parameters are inferred using Bayesian updating, where prior distributions are combined with observed data through a likelihood function to obtain posterior distributions. The likelihood function represents the probability of the observed temperature values given the parameters of the assumed distribution. The observed data is obtained from the uncertainty analysis performed using the TRACE code, which provides the figures of merit for the Bayesian inference process. Once the posterior distributions of the parameters are obtained, a posterior predictive distribution is derived, which quantifies the uncertainty in PCT predictions. This predictive distribution is then used to estimate the probability of exceeding the critical threshold, thereby assessing the likelihood of failure. Since this process generates a distribution of parameters that characterize the predictive distribution of PCT, it allows for the quantification of the uncertainty distribution of the probability of failure.

A critical aspect of Bayesian inference is the choice of prior distributions, which influence model performance and interpretability. This study employs non-informative (NI) and weakly informative (WI) priors to facilitate inference when prior knowledge is limited, ensuring numerical stability while allowing the data to shape the posterior distribution. The failure probability quantification is implemented using the PyMC library in Python, using the Markov Chain Monte Carlo (MCMC) approach [17]. The results of this analysis are summarized in Table 2.

Table 2. Probability Quantification of Natural Circulation Failure

Model*	Likelihood function	Prior distribution	Posterior distribution	Predictive distribution	Q_{ICS}[-]
Inv.CDF	N/A	N/A	N/A	N/A	0
Normal (N) NI	N(μ,σ)	μ~U(550,3000) σ~HF	μ,σ estimated via MCMC	Generated from N(μ,σ)	Mean 0 with range [0,0]
Log-Normal (LN) NI	LN(μ,σ)	μ,σ~ HF	μ,σ estimated via MCMC	Generated from LN(μ,σ)	Mean 0 with range [0,0]
Gamma (G) NI	G(α,β)	α,β~ HF	α,β estimated via MCMC	Generated from G (α,β)	Mean 0 with range [0,0]
Normal (N) WI	N(μ,σ)	μ~N(900,400) σ~HN(300)	μ,σ estimated via MCMC	Generated from N(μ,σ)	Mean 0 with range [0,0]
Log-Normal (LN) WI	LN(μ,σ)	μ~N(log(900),0.5) σ~ HN (0.5)	μ,σ estimated via MCMC	Generated from LN(μ,σ)	Mean 0 with range [0,0]
Gamma (G) WI	G(α,β)	α~G(2,0.01) β~G(2,0.01)	α,β estimated via MCMC	Generated from G (α,β)	Mean 0 with range [0,0]

In all cases the probabilities are effectively equal to zero, and the reliability of natural circulation in the BWRX-300 isolation condenser system is assured within the limited scope of the analysis performed.

In practice, however, the complexities involved in the phenomenon of natural circulation and the limited scope of critical parameters analyzed in this project ensure that some uncertainty regarding the reliability of the system must be accounted for. As a result, assigning a probability of zero to natural circulation as a failure mode is inappropriate. To this end, a failure probability of 1.0E-07 is chosen. This value is justified on the basis that it is of the same magnitude as the least likely basic event probability considered in the accompanying PSA (solenoid valve internal rupture, 7.49E-08; see [6]), as well as the result achieved for the reliability of natural circulation in a passive decay heat removal system in the paper by So & Kim (6.14E-08) [14].

Furthermore, in the TRACE model used to simulate ICS operation and the associated reliability assessment, only a single train is considered, which represents the system requirement 1 out of 3 ICS trains. Thus, the final result for the unavailability of natural circulation can only be strictly applicable to a single loop. Additionally, it has been assumed that the likelihood of natural circulation failure decreases as the number of loops in operation increases. This assumption greatly simplifies the analysis, as the natural circulation failure per each ICS train can be modeled by a set of three basic events, each placed within the fault trees for the operation of each loop. This approach avoids the need to simulate both two and three loops operating simultaneously. However, additional TRACE simulations

* N – Normal, LN – LogNormal, G – Gamma, U – Uniform, HN – HalfNormal, HF - HalfFlat. For the numerical implementation and description of these distributions, refer to [17].

considering the simultaneous operation of several ICS trains are necessary to confirm this assumption, which is outside the scope of this work.

4.2. ICS Unavailability

Failure mode and effect analysis was performed to determine the basic events by which the safety function of the ICS might be impaired. These basic events, as well as their frequencies, are tabulated in Appendix D of [8]. The dependency of successful core cooling and pressure control on the basic events determined by FMEA was used to form fault trees. These were constructed using RiskSpectrum® PSA software, the full results of which may also be found in Appendix D of [8]. An abridged fault tree for a single ICS loop, as well as for the system as whole for the conditions of all three loops or only two loops being available, are shown in Figure 4. The fault trees for all three loops (A, B, and C) are identical, except that only one loop has the possibility of being unavailable due to maintenance. Several component failure modes which could lead to system failure were not modeled. These, and the basis for their omission, include:

- A rupture of the ICS pool or the obstruction of the pool vent path, which is assumed improbable without a major external event, and thereby is outside the scope of this analysis.
- System piping rupture, or the rupture of any of the system components, which may be considered as an initiating event due to plant consequences. This was considered to be within the ICS Line Break initiating event of the accompanying PSA in [8].
- Failure of ICV-5 to operate due to loss of power is not considered [8].

System unavailability was calculated for initiating events where all three system loops are considered 'available', Q_3 , to be 2.54E-07; this case explicitly considers the possibility that one loop may be in maintenance. If only two loops are available, due to the catastrophic failure of one loop, such as in an ICS line break, Q_2 = 4.08E-05. As stated, the probability that a loop is unavailable due to such a catastrophic failure is considered as an initiating event (i.e. a loss of coolant accident) and is accounted for within the frequency of such an event occurring and the successful operation of the ICS isolation valves. Failure to isolate the affected ICS train leads to core damage. See the accompanying PSA in [8]

The largest contributing minimal cutsets to Q_3 are:

- CCF of all heat exchangers (15.70% - 1 cutset),
- Spurious isolation of 2oo3 loops due to isolation valve signal failure and maintenance on the third loop (56.6% - 48 cutsets)
- Spurious isolation of all loops due to isolation valve signal failure (24.96% - 64 cutsets).

The largest contributing minimal cutsets to Q_2 are:

- Spurious isolation of a loop due to isolation valve signal failure with remaining loop in test or maintenance (58.88% - 8 cutsets).
- Spurious isolation of both loops due to isolation valve signal failure (39.20% - 16 cutsets).

Similar results can be observed in the sensitivity analysis results, where the basic events that represent maintenance, isolation valve signal failure and CCF in heat exchanger have the Fussel-Vessely[†] (FV) measures equal to 19.4%, 16.0% and 15.7% respectively. At the same time FV measures for the failure of natural circulation is equal to 0.0016% (per basic event).

For comparison, the failure probability of the ESBWR ICS is 2.13E-03. This disparity is accounted for due to requiring 2 of 4 loops to operate, in contrast to the 1 of 3 requirement for the BWRX-300. Additionally, the value used for loop unavailability due to test or maintenance in this analysis was taken from NUREG/CR-6928 (2020 Update) [13], which is nearly an order of magnitude lower than that used for the ESBWR (3.05E-03 vs 3.84E-02). This is crucial, as loop unavailability due to maintenance, concurrent with the spurious operation of a loop isolation valve, accounts for 86.4% of ICS unavailability in the ESBWR design [6].

[†] The Fussel-Vesely importance measure for a basic event A_i is defined as the conditional probability that the top event (system failure) occurs given that A_i occurs. Fussell-Vessely importance measure can be expressed as follows: $I_{FV}(A_i) = Q(Top\ event\ \&\ A_i)/Q(Top\ event)$[16].

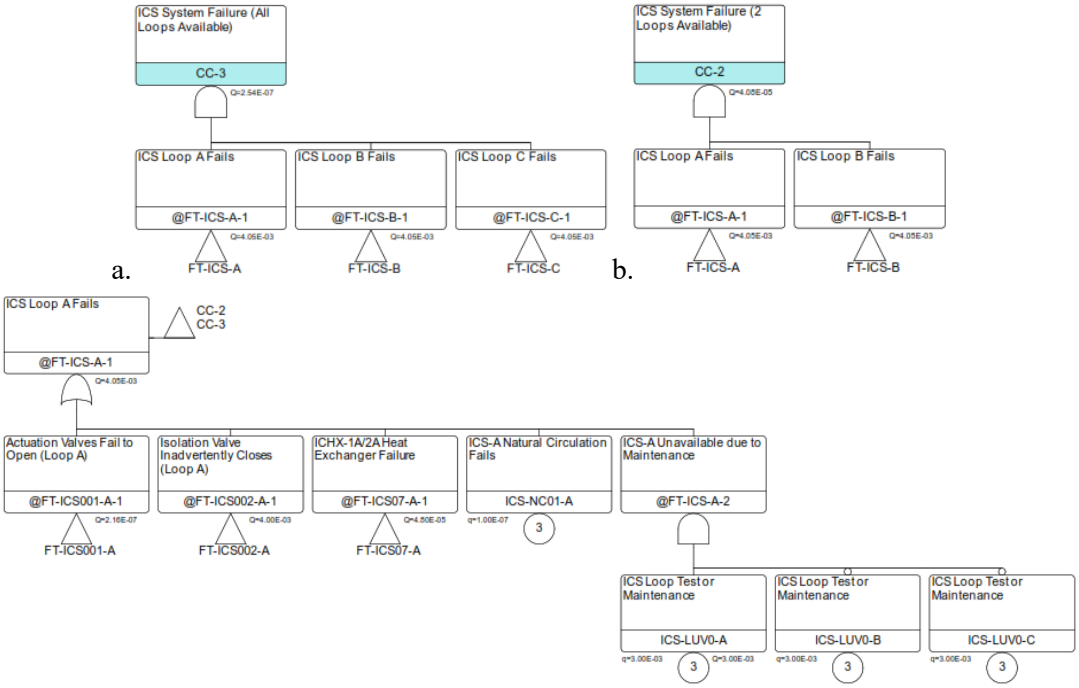

Figure 4 Abridged fault trees for ICS system failure (in cases of two or three loops available), as well as for a single loop [8].

4.3. Core Damage Frequency Analysis

A consequence analysis for event sequences resulting in core damage was performed using the RiskSpectrum® PSA software, resulting in a Core Damage Frequency (CDF) of 1.67E-07 yr^{-1}. Insights gained from the top 100 most influential minimal cutsets to core damage frequency according to the system/component failures involved or the causative initiating event category show that the failure modes involving the ICS are overwhelmingly the source of core damage, accounting for 95.31% of the CDF. From the perspective of initiating events, the transient initiating event category makes the largest contribution to the CDF, which can be attributed to the relative likelihood of a transient compared to other initiating event groups (refer to [8] for more details).

A simplified sensitivity analysis was conducted by increasing the failure probability of natural circulation by 100-fold to 1.00E-05, showed that it leads to only 0.6% increase in the core damage frequency. Thus, it can broadly be concluded from this simple sensitivity analysis that the reliability of natural circulation has a relatively low impact on CDF within these ranges.

It should be noted that the current analysis considers independent failures of natural circulation in each ICS loop separately, without accounting for CCF affecting natural circulation in two or more loops.

5. CONCLUSIONS

A reliability assessment was performed of the BWRX-300 ICS using the RMPS methodology and Bayesian inference, which verified the robust operation of the design during a reactor trip transient. In acknowledgment of the residual uncertainty remaining regarding natural circulation as a failure mode, an unavailability of 1E-07 was assigned. This value was integrated into a FMEA of the ICS, allowing for determination of the total system unavailability. In the standard case that all three ICS loops are available, unavailability was found to be 2.54E-07.

In conclusion, the RMPS methodology and Bayesian inference thus provides a simple and intuitive way to quantify passive system reliability, further creating a framework that readily integrates into current approaches to the safety analysis of nuclear systems.

REFERENCES

[1] A. Saltelli, S. Tarantola, F. Campolongo, and M. Ratto, Sensitivity Analysis in Practice: A Guide to Assessing Scientific Models, Wiley, 2004.

[2] S. Galushin, D. Grishchenko, P. Kudinov, Implementation of framework for assessment of severe accident management effectiveness in Nordic BWR, Reliability Engineering & System Safety, Volume 203, 2020.

[3] Burgazzi, L., Addressing the challenges posed by advanced reactor passive safety system performance assessment, Nuclear Engineering and Design, Volume 241, Issue 5, 2011.

[4] M. Marquès, J.F. Pignatel, P. Saignes, F. D'Auria, L. Burgazzi, C. Müller, R. Bolado-Lavin, C. Kirchsteiger, V. La Lumia, I. Ivanov, Methodology for the reliability evaluation of a passive system and its integration into a Probabilistic Safety Assessment, Nuclear Engineering and Design, Volume 235, Issue 24, 2005.

[5] IAEA TECDOC-1752, Progress in Methodologies for the Assessment of Passive Safety System Reliability in Advanced Reactors, IAEA, 2014

[6] GE Hitachi Nuclear Energy, ESBWR Certification Probabilistic Risk Assessment, NEDO-33201 Revision 6. GE-Hitachi Nuclear Energy Americas LLC, 2010

[7] GE Hitachi Nuclear Energy, Ontario Power Generation Inc. Darlington New Nuclear Project: BWRX-300 Preliminary Safety Analysis Report, NEDO-33950 Revision 2. GE-Hitachi Nuclear Energy Americas, LLC, 2022. Accessed: May 26, 2023. [

[8] G. Trundle, 'Reliability Assessment of Passive ICS in an SMR as part of the PSA Analysis', Master Thesis Report, KTH/NPS, 2023.

[9] Status Report - BWRX-300." International Atomic Energy Association, 2019.

[10] G. Trundle, S. Galushin, S. Roshan, M. Söderström, S. Betcha, and A. Olsson, Reliability Assessment of the BWRX-300 Passive Isolation Condenser System: Addressing Uncertainties in Two-Phase Natural Circulation Flow Modeling, 21st International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-21), August 31-September 5, South Korea, Busan, 2025.

[11] Uncertainty Analysis User's Manual: Symbolic Nuclear Analysis Package (SNAP), Version 1.8.1. Applied Programming Technology, Inc., 2022

[12] G. Trundle, S. Galushin, S. Roshan, M. Söderström, S. Betcha, and A. Olsson, "Reliability Assessment of Passive Isolation Condenser System of the BWRX-300," presented at the 17th International Conference on Probabilistic Safety Assessment and Management & Asian Symposium on Risk Assessment and Management (PSAM17&ASRAM2024), Miyagi, Japan, Oct. 2024.

[13] Idaho National Laboratory, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants (2020 Update), NUREG/CR-6928. U.S. Nuclear Regulatory Commission, 2007.

[14] E. So and M. C. Kim, "Level 1 probabilistic safety assessment of supercritical–CO2–cooled micro modular reactor in conceptual design phase," Nuclear Engineering and Technology, vol. 53, no. 2, pp. 498-508, 2021

[15] P. Kral, J. Hyvärinen, A. Prošek, and A. Guba, "Sources and Effect of Non-Condensable Gases in Reactor Coolant System of LWR," presented at the 16th International Topical Meeting on Nuclear Reactor Thermal Hydraulics (NURETH-16), Chicago, IL, Sep. 2015

[16] M. Modarres, M. Kaminskiy, V. Krivtsov, Reliability Engineering and Risk Analysis: Practical Guide, Marcel Dekker, New York, ISBN: 0-8247-2000-8, 1999

[17] PyMC, "PyMC: Probabilistic Programming in Python," 2025. [Online]. Available: https://www.pymc.io. [2026-05-02]