Reliability Assessment of Passive Isolation Condenser System of the BWRX-300

Graeme Trundle[a*], Sergey Galushin[b], Sean Roshan[a]
Michael Söderström[c], Sevostian Bechta[a] Anders Olsson[b]
[a]Royal Institute of Technology (KTH), Stockholm, Sweden (trundle@kth.se, sean@safety.sci.kth.se, bechta@safety.sci.kth.se)
[b]Vysus Group, Stockholm, Sweden (sergey.galushin@vysusgroup.com, anders.olsson@vysusgroup.com)
[c]Vattenfall AB, Stockholm, Sweden (michael.soderstrom@vattenfall.com)

Abstract: Passive safety systems are increasingly being utilized in prospective nuclear power plant designs. The low magnitude of the forces involved in such systems, combined with the uncertainty inherent in the factors which affect them, pose a problem in the assessment of their reliability when compared to their active counterparts.
The purpose of this paper is to investigate and apply a state-of-the-art technique in passive reliability assessment, known as the Reliability Methods of Passive Systems (RMPS) methodology, to the isolation condenser system (ICS) of the prospective BWRX-300 small modular reactor (SMR) design. The ICS is a safety system driven by natural circulation which provides emergency core cooling and pressure control for the BWRX-300. Using RMPS to analyze the effect that uncertainties in thermal characteristics of the fuel have on ICS operation, the reliability of natural circulation was quantified with a confidence of 99%.
This yielded an immeasurably small failure probability. Considering residual uncertainty, an engineering judgment assigned a failure probability of 1.00E-07. This finding was integrated into a fault tree analysis of the ICS using failure mode and effect analysis (FMEA) of system components, including insufficient natural circulation as a failure mode. Analysis of sequences leading to failure resulted in system unavailability being determined as 1.62E-07 for the case of all three loops initially available, and 2.91E-05 for the case when only two loops are initially available.

Keywords: Passive system reliability, Reliability Methods of Passive Systems, Natural circulation, TRACE, RiskSpectrum PSA.

1. INTRODUCTION

Passive safety systems are 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 [1]. 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.

This paper utilizes the Reliability Methods for Passive Systems (RMPS) methodology to perform a simplified reliability assessment of a passive safety system for the BWRX-300, a small modular reactor developed by GE Hitachi Nuclear Energy (GEH). The safety system chosen is the Isolation Condenser System, responsible for providing core cooling and pressure control when normal means are unavailable; the latter duty is owed to GEH's novel omission of safety relief valves, which is stated as the most likely cause of a loss of coolant accident [9]. These responsibilities are accomplished using natural circulation as a motive force, whereby decay heat is transferred to the atmosphere by three independent heat exchanger loops through the evaporation of system pool water. See Figure 1 below.

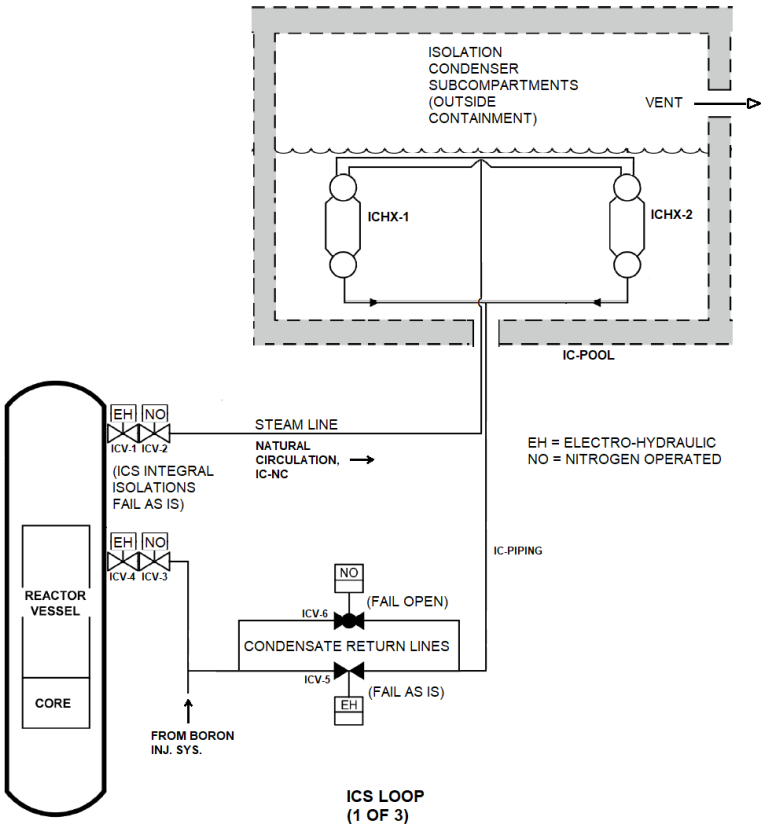

Figure 1. The BWRX-300 Isolation Condenser System, adapted from details provided in [4] and [5].

2. METHODOLOGY

The reliability of natural circulation as a motive force for the BWRX-300 ICS was assessed using a simplified variation of the RMPS methodology. The choice of this methodology is justified according to its ease of integration into traditional fault tree analysis and the relatively large body of research available regarding its application to natural circulation systems [2,3]. Accordingly, an assessment of the ICS as a whole was also performed, incorporating natural circulation as a possible failure mode. As such, the following steps were performed in this analysis:

1. The BWRX-300 ICS was modeled in TRACE, a two-fluid thermal-hydraulic code developed by the Nuclear Regulatory Commission (NRC) for the deterministic safety analysis of nuclear systems. This is comprised of a transient model which simulates a simple reactor trip, requiring ICS operation.
2. System acceptance criteria were identified by reference to the ESBWR safety analysis performed by GEH [4].
3. Parameters which have the largest influence on system success in preventing failure criteria from being met, so-called critical parameters, were identified using engineering judgment and by reference to previous reliability assessments, specifically by So & Kim [3].
4. Probability distribution functions were assigned to the key parameters, in a fashion likewise to step 3.
5. The TRACE transient model was run iteratively with random sampling of critical parameters according to the previously mentioned probability distribution functions using the SNAP uncertainty plug-in. The number of iterations was calculated using Wilks' formula for a first order 95% tolerance and 99% confidence interval [12].
6. The probability for the failure of natural circulation to sufficiently occur within an ICS loop was determined from the mean and standard deviation of the resultant acceptance criteria parameters, assuming they obey a Gaussian distribution according to the central limit theorem. The reliability of natural circulation may then be said to be quantified by this failure probability, which may be used in a conventional fault tree analysis as a basic event for ICS failure.
7. A reliability assessment of the ICS was performed using FMEA to identify critical component failure modes, including those from dependencies of interfacing systems, common cause failures, and natural circulation. Using RiskSpectrum PSA, a risk and reliability software suite developed by RiskSpectrum

AB, a fault tree model of the ICS was developed, and further integrated into a Level 1 probabilistic safety analysis of the BWRX-300 in the accompanying work [6].

2.1. BWRX-300 Reactor Trip Transient Simulation

A transient simulation was performed to model a reactor scram at full power, requiring actuation and operation of a single ICS loop to maintain system temperatures and pressure within specification. The approach to modeling the reactor scram was taken from Pomogaev [7], whereby decay heat was varied according to:

$$Q_D(t) = 0.0657 Q_0 t^{-0.2} \quad (1)$$

for initial power Q_0 (870 MWth) and time after shutdown t. It was assumed that 5 seconds were required to fully insert control rods, with an additional 1 second delay to simulate scram logic actuation. Thus, a total of 6 seconds occurred between the point when the scram was required (transient start time) to when decay heat was simulated according to Eq. 1; over this period, reactor power was conservatively assumed to remain constant at Q_0. Model details of note include:

- The power profile was modeled axially according to a cosine function and radially flat.
- The RPV was simulated to be isolated concurrently with the reactor scram. This was modeled by shutting the RPV isolation valves (RPVIVs) at their fastest speed, which is expected to be conservative. RPVIV shutting times were taken to be the same as the main steam isolation valves (MSIV) and feedwater isolation valve (FWIV) shutting times for the ESBWR. At their fastest, these times are three seconds and ten seconds for the MSIV and FWIV, respectively [8].
- Operation of the single ICS loop was simulated by opening both condensate return actuation valves (ICV-5/6) simultaneously. The actuation valve opening time was set as the slowest of those associated with the ESBWR ICS, with an additional one second logic delay. To this end, the actuation valves commence opening one second after the start of the transient and completed opening 30 seconds later [8].
- Credit is not taken for the availability of the feedwater pumps powered from the electrical grid. Thus, feed pumps are simulated to be lost at the start of the transient. This is modeled by feedwater flow decreasing linearly over four seconds to simulate pump coast down.
- Finally, the ambient temperature and pressure of the IC pool was conservatively set to 373 K and 0.11 MPa.

Further details, including geometric input data and nodalization scheme used, are found in [6]. The maximum calculated values for system parameters of note, denoted ‘peak’ parameters, are presented below in Table 1, as well as for 24 hours after the start of the transient.

Table 1. Peak Parameters following BWRX-300 Reactor Trip Transient [6]

Parameter	Maximum	24 Hours
Peak vessel pressure	7.8220 MPa	482.79 kPa
Peak cladding temperature	567.40 K	415.80 K
Peak fuel temperature	1192.5 K	418.79 K

2.2. Acceptance Criteria

The acceptance criteria used to judge the successful operation of the BWRX-300 isolation condenser system will be defined by reference to those used in the ESBWR PRA [4]. For this analysis, the following criteria will thus define successful ICS operation:

1. RPV pressure remains below 150% of the design pressure, 15.45 MPa [5].
2. Peak cladding temperature is maintained below 1204 °C.

As can be seen from Table 1, the baseline model remains well within these acceptance criteria.

2.3. Critical Parameters

The critical parameters, and the probability distributions associated with their uncertainty, were chosen by reference to a similar study for a residual heat removal system performed by So & Kim [3], as well as by

experimentation of parameters which had a large impact on peak system pressure during the transient. Further, all critical parameters chosen are temperature-dependent thermal characteristics of the fuel rods, which are evaluated for by TRACE. Thus, their uncertainty was modeled by a scaling factor according to a normal distribution. The parameters and associated probability distributions are shown in Table 2 below.

Table 2. Critical Parameters and Distribution [6]

Parameter	**Distribution**
Gas gap thermal conductivity	Normal ($\mu = 1.0$, $\sigma = 0.102043$), scaling factor
Fuel thermal conductivity	
Cladding thermal conductivity	
Fuel specific heat capacity	
Cladding specific heat capacity	

2.4. ICS Reliability Assessment

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 [4]; this additionally precludes any consideration that failed system components are repaired over this period. Further, only basic events internal to the system were considered.

2.4.1. 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 [9].

2.4.2. 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).

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 [5], 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) [4].

2.4.3. 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. Thus, a loss of power is not considered a relevant failure mode within the scope of this analysis.
- 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 [4].

2.4.4. 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 [4], 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 [6].

3. RESULTS

The transient model was run iteratively while individually sampling the critical parameters according to the distribution found in Table 2. To this effect, dependencies between the critical parameters were not modeled. Sampling was performed using the built-in SNAP uncertainty plug-in. Using Latin Hypercube Sampling, 130 iterations were simulated to reach a 99% confidence in the results; this was determined according to the Wilks' method, computed automatically by DAKOTA [10].

Table 3. Acceptance Criteria Output Distributions [6]

Parameter	**Normal Dist. Parameters (μ, σ)**
Peak system pressure	(7.8328 MPa, 87.5 kPa)
Peak cladding temperature	(567.59 K, 0.70 K)

The resulting distributions for the acceptance criteria parameters, PCT and pressure, are tabulated in Table 3. The horsetail plots, probability densities, and cumulative distribution histograms are seen in Figure 2. The probability that either acceptance criterion is violated due to the uncertainty in the critical parameters of Table 2 was numerically calculated by evaluating the inverse cumulative distribution function for each criterion at their respective allowable limits and using the inclusion-exclusion principle, conservatively assuming that the probability of either event is independent. Based on the distributions for both PCT and pressure presented in Table 3, this probability falls below the computable limit. Therefore, these probabilities are taken to be effectively zero, and the reliability of natural circulation in the BWRX-300 isolation condenser system is assured within the limited scope of the analysis performed.

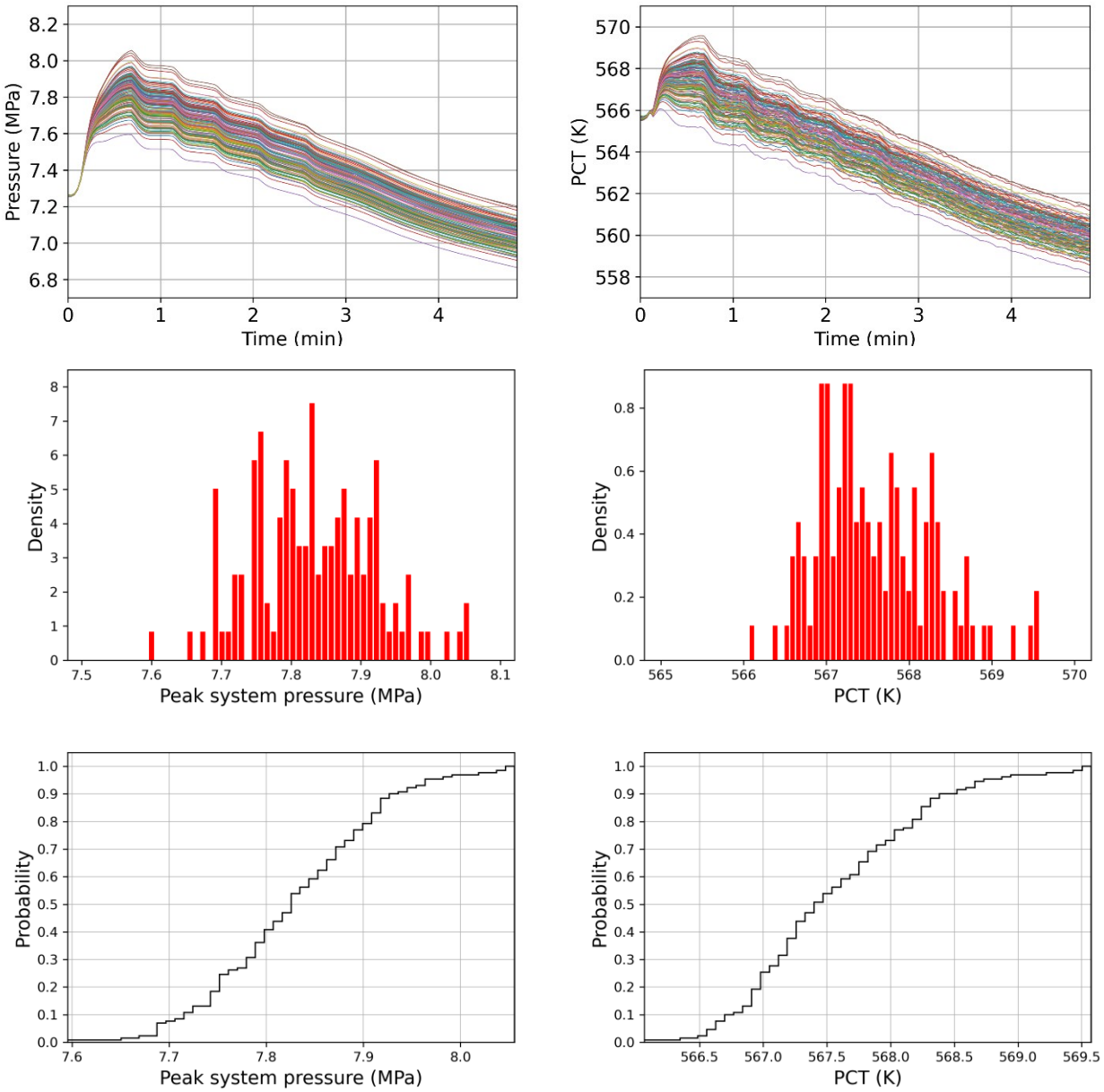

Figure 2. Horsetail plots (top), probability density functions (center) and cumulative distribution functions (bottom) for peak system pressures (left) and peak cladding temperatures (right) [6].

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 1E-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) [3].

An important limitation of this reliability assessment, particularly regarding its application in a PSA, is the lack of variation in casualty scenarios analyzed. Ideally, the performance of the ICS would be modeled for every initiating event considered in the PSA. The transient modeled in this assessment, i.e., a simple reactor trip, should not be considered a bounding scenario in terms of severity. Thus, for proper implementation in a PSA, further analysis is required which is outside the scope of this work.

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,

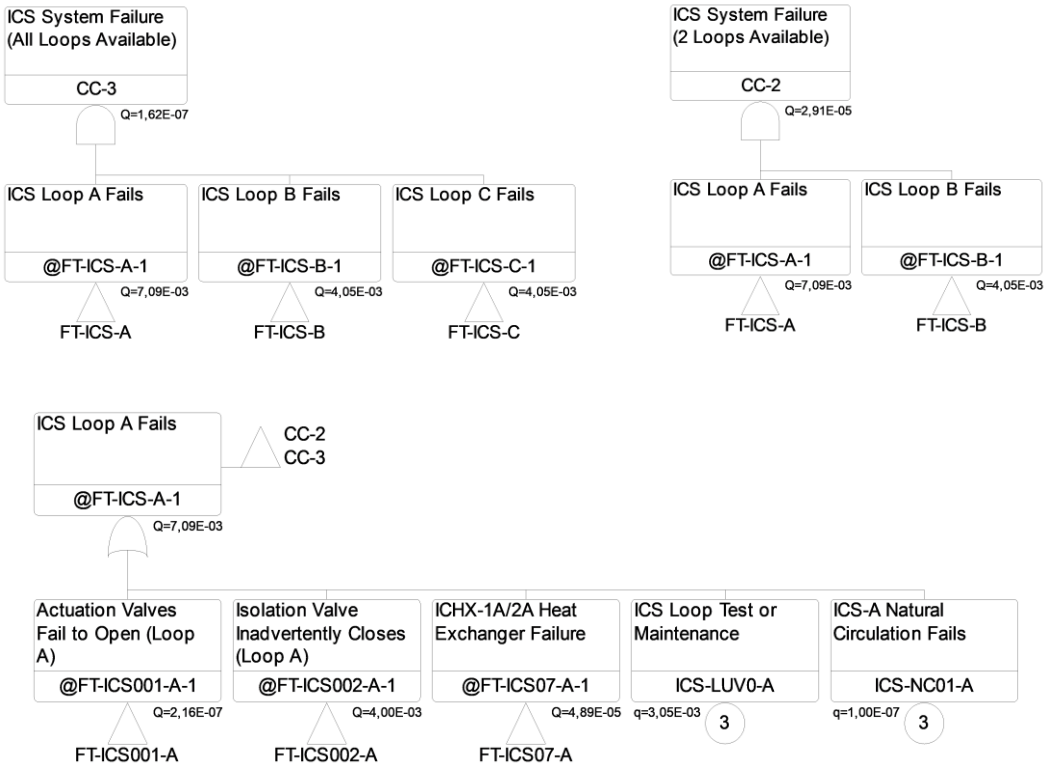

Figure 3. Abridged fault trees for ICS system failure (in cases of two or three loops available), as well as for a single loop [6].

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

Regardless, for the sake of investigating the integration of a passive reliability assessment into a traditional PSA, the failure probability determined for natural circulation will be considered as a failure mode in the Failure Mode and Effect Analysis (FMEA) performed for the ICS below. This will permit the formation of an ICS fault tree, allowing for calculation of the total unavailability of the system.

3.1. 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 [6]. 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 software, the full results of which may also be found in Appendix D of [6]. 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 3. The fault trees for all three loops (A, B, and C) are identical, except that only a single loop, loop A, 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 [6].
- Failure of ICV-5 to operate due to loss of power is not considered (see section 2.4.3).

System unavailability was calculated for initiating events where all three system loops are considered 'available', Q_3 , to be 1.62E-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 = 2.91E-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 [6].

The largest contributing minimal cutsets to Q_3 are:

- Common cause failure of all heat exchangers (34.75%),
- Spurious isolation of all loops due to isolation valve signal failure (34.56%), and
- Spurious isolation of two loops due to isolation valve signal failure with the remaining loop in test or maintenance (26.08%).

The largest contributing minimal cutsets to Q_2 are:

- Spurious isolation of both loops due to isolation valve signal failure (54.88%), and
- Spurious isolation of a loop due to isolation valve signal failure with remaining loop in test or maintenance (41.88%).

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) [11], 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 [4].

3.2. 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 1.23E-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 [6] 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 0.41% 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.

4. CONCLUSIONS

A reliability assessment was performed of the BWRX-300 ICS using the RMPS methodology, 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 1.62E-07.

In conclusion, the RMPS methodology 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. Further, the BWRX-300, using the passive isolation condenser system, represents an innovative platform that robustly addresses challenges to plant safety in a cost-effective manner.

References

[1] "Use of Passive Safety Features in Nuclear Power Plant Designs and their Safety Assessment." https://www.iaea.org/topics/design-safety-nuclear-power-plants/passive-safety-features (accessed Jun. 13, 2023).

[2] J. Jafari, F. D'Auria, H. Kazeminejad, and H. Davilu, "Reliability evaluation of a natural circulation system," Nuclear Engineering and Design, vol. 224, no. 1, pp. 79–104, 2003, doi: https://doi.org/10.1016/S0029-5493(03)00105-5.

[3] 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, doi: https://doi.org/10.1016/j.net.2020.07.029.

[4] GE Hitachi Nuclear Energy, ESBWR CERTIFICATION PROBABILISTIC RISK ASSESSMENT, NEDO-33201 Revision 6. GE-Hitachi Nuclear Energy Americas LLC, 2010. Accessed: May 26, 2023. [Online]. Available: https://www.nrc.gov/docs/ML1028/ML102880548.pdf

[5] 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. [Online]. Available: https://www.opg.com/documents/dnnp-bwrx-300-preliminary-safety-analysis-report.pdf/

[6] G. Trundle, 'Reliability Assessment of Passive ICS in an SMR as part of the PSA Analysis', Master Thesis Report, KTH/NPS, 2023. [Online]. Available: https://kth.diva-portal.org/smash/get/diva2:1787404/FULLTEXT01.pdf

[7] A. Pomogaev, "BWRX-300 isolation condenser system analysis." Lappeenranta–Lahti University of Technology, 2022. Accessed: May 31, 2023. [Online]. Available: https://lutpub.lut.fi/bitstream/handle/10024/164715/Pomogaev_thesis.pdf?sequence=1&isAllowed=y

[8] GE Hitachi Nuclear Energy, ESBWR Design Control Document, Tier 2, Revision 10. GE-Hitachi Nuclear Energy Americas, LLC, 2014. Accessed: May 25, 2023. [Online]. Available: https://www.nrc.gov/reactors/new-reactors/large-lwr/design-cert/esbwr.html

[9] "Status Report -- BWRX-300." International Atomic Energy Association, 2019. Accessed: May 2023. [Online]. Available: https://aris.iaea.org/PDF/BWRX-300_2020.pdf

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

[11] 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. [Online]. Available: https://nrcoe.inl.gov/publicdocs/AvgPerf/AvgPara2020.pdf

[12] N. W. Porter, Wilks' Formula Applied to Computational Tools: A Practical Discussion and Verification, SAND2019-1901J