Benchmark on dynamic PRA with simplified decay heat removal system model of sodium fast reactor – Part 2 (DPRA problem description and benchmark results)

Christoph Döderlein[a*], Koki Ihara[b], Atsushi Matsumoto[c], Hidemasa Yamano[d], Akihiro Shibata[e]
[a]French Alternative Energies and Atomic Energy Commission (CEA), Cadarache, France
[b]Mitsubishi Heavy Industries Ltd. (MHI), Hyogo, Japan
[c]MHI NS Engineering (MHINSE), Hyogo, Japan
[d]Japan Atomic Energy Agency (JAEA), Oarai, Japan
[e]MITSUBISHI FBR SYSTEMS, INC. (MFBR), Tokyo, Japan

Abstract: Decay heat removal systems (DHRS) in sodium-cooled fast reactors (SFR) exhibit unique characteristics, such as long mission times, substantial grace periods, and complex interdependencies. These features render them particularly well-suited for the application of dynamic probabilistic risk assessment (DPRA) methods for accurate reliability evaluation. In this study, we benchmark two DPRA methods developed in Japan and France using a simplified version of the DHRS for the ASTRID reactor.

While the first part of this study validated the thermal hydraulic models across different scenarios, the present paper elaborates on the probabilistic analysis conditions, outlines the different calculation approaches, and compares the results of the benchmark cases.

Keywords: dynamic PRA, decay heat removal system, sodium fast reactor, fast breeder reactor.

1. INTRODUCTION

The safety studies of Sodium cooled Fast Reactors (SFR) must consider the possibility of a total and prolonged loss of the Decay Heat Removal Systems (DHRS), as this event could lead to the inacceptable failure of the core support structures. However, the specific characteristics of an SFR type reactor make conventional approaches to estimate the probability of a complete and prolonged loss of the DHRS function over long periods, known as "static PRA", unsuitable. On the one hand, the long duration of the considered mission time (1000 h and more) and the redundant and diversified nature of the DHRS equipment allow for the consideration of the repair of failed components, crucial for avoiding an overly pessimistic reliability assessment. The significant thermal inertia of the sodium coolant coupled with the rapidly decaying decay heat during a hypothetical accident transient introduces time-dependent factors that are inadequately captured in static event trees, resulting in overly conservative static PRA estimates.

To address the limitations of conventional probabilistic risk assessment (PRA) methods and facilitate the demonstration of the practical elimination of prolonged decay heat removal system (DHRS) failures, dynamic PRA (DPRA) approaches have been developed. This paper, together with its first part [1], presents a benchmark of DPRA approaches developed in Japan and France, applied to a simplified DHRS model of the ASTRID reactor project [2].

The simplified model used for the comparative study of the dynamic approaches is described in detail in [1]. This simplified model represents the two DHRS systems, S1 and S2, each composed of two trains. System S1 is a forced convection system, while S2 evacuates decay heat through natural convection and radiation from the main vessel. The presentation [1] describes in detail the DHRS and its physical properties as represented in the physical models of the two DPRA approaches, along with the corresponding benchmark results.

This document presents in chapter 2 the probabilistic modeling of the DHRS and its support systems, including inter-system dependencies and common cause failures (CCFs), as represented in a static RiskSpectrum® [3] model. This chapter further details the dynamic characteristics of the simplified model, including time-dependent modeling of failures and repairs. Chapter 3 outlines the Japanese and French computational approaches. Chapter 4 presents the benchmark program, encompassing the initiating scenario, analyzed cases, and comparative results of the different methods. The concluding Chapter 5 summarizes findings and explores potential avenues for future research.

2. PROBABILISTIC CARACTERISTICS OF THE SIMPLIFIED MODEL

2.1 Static probabilistic model

The static probabilistic modeling was based on the one developed for ASTRID which was designed to enhance the consistency and reliability of DHR systems design with regard to redundancy and diversification, to assess the balance between scenario contributions and to identify functional dependencies between safety systems, with the ultimate goal of evaluating the core damage frequency for protected and unprotected sequences.

The benchmark model was simplified compared to the ASTRID reference configuration by excluding the third in-vessel DHRS and the DHR functions of the secondary sodium loops. Additionally, the fault tree model incorporated certain simplifications.

The fault tree modeling of the static model is based on conceptual design information, reliability data and common cause failure representation:

- The fault trees for Decay Heat Removal, Electric Power Supply and Instrumentation and Control (I&C) systems were developed using the design information of the simplified model (i.e., in particular, neglecting the third diversified DHRS that was not represented in the benchmark model).
- The reliability data for the components failure rates and probabilities per demand were extracted mainly from the EG&G database [5] for components specific to sodium fast reactor design and from NUREG/CR-6928 [6] for general support systems components.
- Common cause failures on identical redundant equipment in the two trains of each system were modelled using the Multiple Greek Letters approach. No common cause failure is postulated between the two DHR systems.
- Maintenance operations are modelled based on the assumption that preventive maintenance cannot concern more than one DHR train at the same time and renders this train unavailable for a week.
- Human reliability was considered with an arbitrary and conservative probability of 10^{-1} for actions related to the recovery of I&C failures when starting the S2 system.

The modeled equipment is comprised of various components, including pumps, heat exchangers, flaps, and dampers for the Na/air heat exchangers, as well as electrical equipment such as emergency diesel generators, switchboards, transformers, and batteries. Additionally, the HVAC equipment for the rooms containing the pumps and electrical equipment is included in the model.

The *decoupling criterion*, chosen to connect the PSA studies with the safety demonstration of the reactor, corresponds to the average primary sodium temperature, which must not exceed 650 °C in order to prevent thermal creep on the core support structures and on the primary vessel. This decoupling criterion has then been translated into two mission success criteria:

- The “minimum requirement” or deterministic criterion, based on the minimum number of available DHRS necessary to fulfill the temperature criterion. Given the decreasing amplitude of the decay heat after scram, this criterion leads to time-staggered requirements:
    - at least 1 S1 train in the period [0, 30 h],
    - at least 1 S1 train or 2 S2 trains in the period [30 h, 102 h],
    - at least 1 S1 train or 1 S2 train in the period [102 h, end of mission].

  This criterion is used in the generic event tree of the static model (c.f. Figure 3 in [1]), stipulating a mission failure whenever a system unavailability leads to a breach of the minimum requirement.

- The “temperature criterion” or dynamic criterion, which applies the mean sodium temperature calculated in the physical model to the decoupling criterion.

2.2 Dynamic properties

The static probabilistic approach is conservative in that it does not allow to explicitly account for the timing or sequencing of events, nor for the system dynamics (i.e., the thermal inertia of the primary loop). If a system fails during a time period, the static approach considers the failure at the beginning of this time period.

The principle of dynamic methodologies, in order to overcome these limitations, is to generate random sequences of failures and repairs of the DHR systems. They are based on the same data as the static fault trees/event trees modeling, except for taking into account the possibility of repair, with additional probabilistic data depending on repair conditions (see below). From the study of a required large number of random sequences of failures and repairs of the available DHR systems, it is then possible to estimate the probability of exceeding the decoupling criterion by the ratio of the number of the sequences leading to exceeding the decoupling criterion to the total number of sequences.

Following the initiation of the transient, the components of the DHRS and its support systems are therefore subject to failures that can be failures on demand or in operation, as well as simultaneous common-cause failures on demand or in operation. The component failures, as defined in the static model, are therefore classified according to their degree of reparability, which is linked to the supposed mean repair time, into three categories:

- easily repairable failures,
- not-easily repairable failures,
- “irreparable” failures (for S1 only, S2 being considered fully repairable).

Easily repairable failures concern faults in the digital control system, power supply, ventilation, certain support systems, etc., with a mean repair time of less than 24 hours (spare parts are considered to be available).

Not-easily repairable failures concern failures in the electro-magnetic pumps, leakage of the Na/Air heat exchangers and failures of dampers and flaps in the S1 circuits, and all failures affecting the S2 circuits.

For the S1 system, the repair is conditioned by the average temperature in the primary sodium circuit which needs to be compatible with working conditions, i.e. inferior or equal to 300 °C. The repair of the S1 trains is furthermore conditioned by the closing of the flaps and the anti-freeze dampers to prevent the sodium from freezing and their staying closed during repair when the circulation pump is out of order. The mean repair time for *Not-easily repairable failures* is taken as 30 days for failures in S1 and 100 hours for failures in S2.

“Irreparable” failures are leaks of the in-vessel heat exchangers and failures that cause sodium freezing in the S1 circuits (i.e. inadvertent opening of dampers and flaps). These failures are considered irreparable because their repair requires the replacement of large components on the sodium circuits within a period of time that is of the order of the mission time (reference value = 1000 hours in the benchmark).

The mean repair time is taken as a mean down time (MDT) and the repair model is associated with an exponential law for all components, with the probability P of having repaired a component failed at t=0 at time t:

$$\mu = \frac{1}{MDT} \quad (1)$$

with

$$P(t) = 1 - e^{(-\mu \times t)} \quad (2)$$

Immediate repair after diagnosis is assumed to be possible (no particular constraint requires deferring the repair procedure) and the MDT is supposed to include all preparatory and follow-up delays.

3. COMPUTATIONAL APPROACHES

3.1. Japanese DPRA approach

MHI has developed the dynamic PRA code, PRIME (Probabilistic Reliability AnalysIs Mitsubishi Engine), considering state changes in safety systems and equipment due to failures and repairs in response to an accident progression. The program has been coded in C++. The overview for this method is shown in Figure 1. The basic feature of this method is that sequences are automatically generated based on the defined basic events in advance and then the reliability of the whole systems is calculated from the results of sequence occurrence probability and physical behavior evaluation using Monte-Carlo method. The physical behavior of each sequence is evaluated by the thermal-hydraulic calculation component hard-coded in PRIME. In response to the benchmark, the thermal-hydraulic calculation component in PRIME has been tuned up to assess the average temperature of the primary sodium depending on the number and type of DHR systems available, resolving the power balance equation (c.f. § 2.4 in [1]).

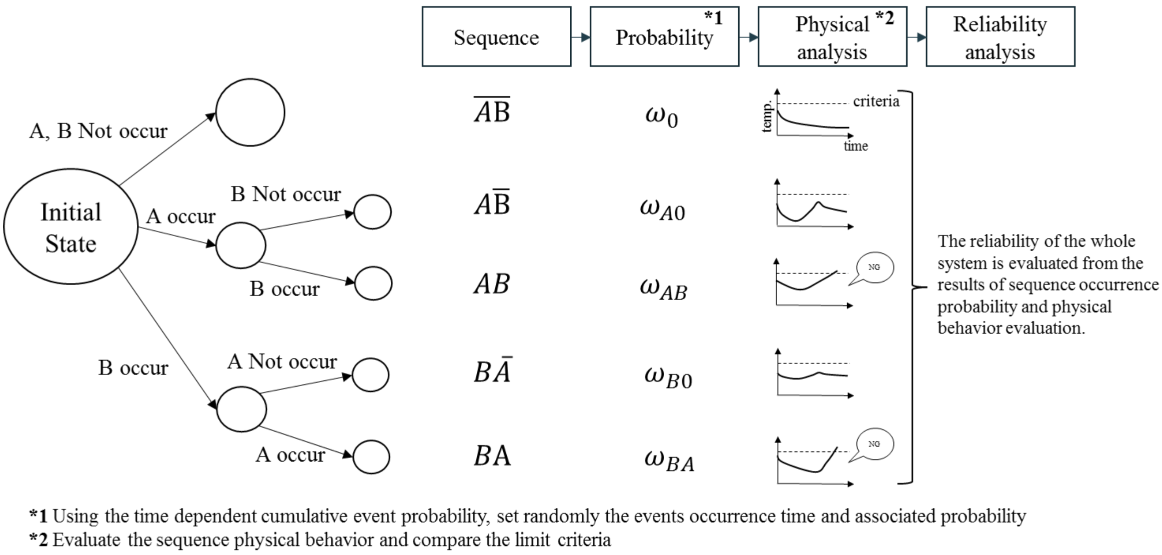

Figure 1. Overview for PRIME

The procedures overview for evaluating overall system reliability using PRIME is described in Figure 2. It starts by setting sequences to be evaluated. First, sequences are generated considering all combinations and orders based on the defined events including the component failures and repairs. Next, sequences are reduced by threshold for the sequence occurrence probability.

After generating sequences, events occurrence time and probability of each sequence are randomly set by using Monte-Carlo sampling. Then the sequence physical behavior of each sample is analyzed using the time dependent system configuration to compare the limit criterion, and samples that excess the limit criterion are flagged. Each sequence reliability is evaluated from the occurrence probability for flagged cases. By calculating each sequence reliability repeatedly in the above way, overall system reliability is calculated as:

$$PE = \frac{\sum_i \sum_j w_{ij}\delta_{ij}}{N} \tag{3}$$

Where,

PE = probability of progression to undesired event, in this benchmark the probability of failure of the DHR function
w_{ij} = probability of sequence j for sampling i
δ_{ij} = event progression flag
(δ_{ijk} = 1 if sequence j for sampling i evolves to undesired event, otherwise δ_{ijk} = 0)
N = the total number of sampling

As an advantage of this method, even events with a low probability of occurrence can be properly evaluated with a relatively small number of trial calculations, by setting the evaluation sequence in advance. Therefore the simulation results can be converged with a relatively small number of samples. In addition, this method has the advantage of identifying dominant failure sequences because it calculates reliability for each sequence. In the benchmark, this feature allows to trace main causes of the mission failure at the level of DHRS and their subsystems. On the other hand, there is an issue in terms of computation time, since a very large number of sequences are evaluated. For an example, for a mission time of 1000 hours in the case with CCF, the execution takes about 15 hours for 1000 samples on Intel(R) Core (TM) i5-8500 CPU @3.00GHz. It should be noted that it is possible to further shorten the execution time by, for instance, deleting unnecessary sequences.

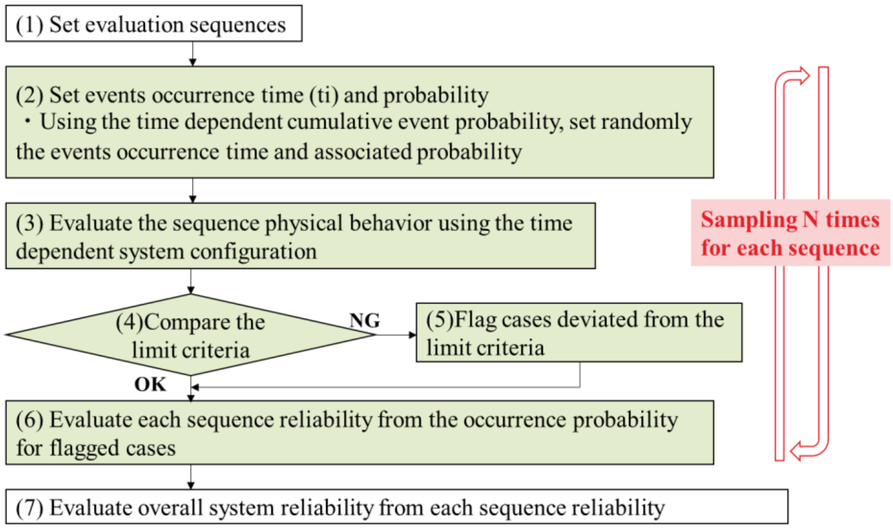

Figure 2. Procedures flow chart for PRIME

3.2. French DPRA approach

Considering the strong conservatism of the static PRA, the dynamic PRA code DayDREAM (DecAY heat removal Dynamic Reliability EvAluation Methodology) has been developed at CEA within the framework of the ASTRID project. The principle of this method is to randomly generate, for each IE considered, sequences of failures and repairs of the available DHRS. It is based, on the one hand, on the fault trees of the DHRS obtained from the static analysis and, on the other hand, on the specific assumptions for the repair times of these systems (cf. § 2.2). For each sequence generated, with the number of operational DHRS known at each point in time, the average temperature of the primary sodium is the assessed using the simplified thermal-hydraulic calculation tool MODENA. By studying a large number of random sequences, the probability of exceeding the decoupling criterion linked to the loss of the DHR function can then be calculated.

The MODENA code has been developed by the CEA [7] to rapidly assess the sodium temperature reached in the primary circuit, depending on the number and type of DHR systems available. This simplified model calculates the mean temperature of primary sodium (T_{mean}) at a given time t by resolving the following heat balance for the main vessel, as described in [1, § 2.4]. The law of evolution of the decay heat as a function of time is represented by a sum of exponentials, the other functions are defined as polynomials. The MODENA code was used as the reference code for the physical model benchmark in [1].

The DayDREAM method operates in a two-step approach: to randomly generate sequences of DHRS failures and repairs, the overall probability of failure of each system is assessed using the static analysis of DHRS fault trees (FT) implemented in the probabilistic model. The two main results of this FT analysis are the overall failure probability during the given mission time of each DHRS and its trains, and the associated Minimum Cut Sets (MCS). The total probability of failure of each system is evaluated, as are the probability ratios of the failure of one train of the two or of the two trains, distinguishing between failures on demand, failures in operation, simultaneous failures (i.e., those caused by a common cause), and non-simultaneous failures.

The MCS represent the set of minimum combinations of failures of elementary components that can cause the system or train to fail. The analysis of the MCSs is then used to consider the nature of the failed components of each MCS in order to evaluate the different types of repair situations (i.e., easily repairable, not-easily repairable or irreparable) and to calculate the probability ratios of the repair situations associated with this system or train failure type. The final result of this step is a multi-dimensional probability matrix for each DHRS, categorizing the failures by trains (1 of 2, both), failure type (on demand, in operation) and repair situation.

The second step of the method consists of generating sequences, based on the probability ratios of the failure types, by a Monte-Carlo simulation in which the randomly drawn variables are the loss times of the DHRS trains (set at t_0 for the on-demand failures and determined by an exponential function for the in-operation failures). Each sequence generated is then analyzed with the MODENA code to determine if the success criterion has been met or not, in which case the sequence is considered *failed*. The ratio of failed sequences to the total number of sequences can then be used to estimate the probability of failure of the DHR function (see below) without repair.

Next, the failed sequences (where the criterion was exceeded) are modified, introducing the repair event. A new random event is therefore introduced to determine the type of repair situation (easily repairable, difficult to repair or irreparable) following the probabilities derived from MCS analysis, and the subsequent time of regaining functionality. The sequences with the updated DHRS availabilities are then re-analyzed with MODENA, the ratio of still failed sequences indicating the DHR failure probability with consideration of the possibility of repair.

The advantage of 'replaying' the failed sequences only is twofold: due to the relatively small number of failed sequences (the failure of the DHR function being a rare event), it is possible to run the repair simulation several times to improve the statistical uncertainty on the effect of the repair possibility. Furthermore, this approach facilitates parametric studies on the repair delays: for each new repair delay, it is sufficient to recalculate only the failed sequences, which saves a substantial amount of calculation time.

The probability of failure of the DHR function, P_f, can then be estimated as the ratio between the number of failed sequences (N_f) and the total number of generated sequences (N):

$$\overline{P_f} = \frac{N_f}{N} \tag{4}$$

The precision of the estimate of this probability is given in terms of the coefficient of variation (*COV*) of the estimate (i.e.: ratio of the standard deviation *SD* to the mean of the estimate), with:

$$\boldsymbol{SD(\overline{P_f}) = \sqrt{\frac{(1-\overline{P_f})\overline{P_f}}{N}}} \tag{5}$$

hence

$$COV(\overline{P_f}) = \frac{\sqrt{\frac{(1-\overline{P_f})\overline{P_f}}{N}}}{\overline{P_f}} \tag{6}$$

The *COV* can serve as convergence criterion. The DayDREAM results presented in this study were obtained with a *COV* of 0.01 (i.e., 1%). The calculation time increases with the mission time. For instance, with a 1000 hour mission time and considering common cause failures (CCFs), achieving a COV of 0.01 for the probability of conditional failure (i.e., in the event of both S1 trains failing) required approximately 200,000 generated sequences.

Originally developed in FORTRAN95, the program was recoded in Python 2.7, with the exception of MODENA, which was retained in its original language for performance optimization. The execution of the aforementioned example consumes approximately 20 minutes on a Xeon® 3.20GHz processor. This computational efficiency facilitates the practical implementation of parametric studies. However, the method is unable to identify dominant failure sequences, i.e., trace the DHRS failure to a specific MCS and thereby pinpoint the equipment or subsystem at the root of the mission failure.

4. BENCHMARK PROGRAM AND RESULTS

4.1. Benchmark transient and analysis cases

Since this study aims to compare the various dynamic approaches in terms of their ability to contribute to the demonstration of the practically eliminated situation of complete and prolonged loss of DHRS function, it is assumed that the considered transient is initiated by the occurrence of a "generic" initiating event (IE). This generic IE represents any event that does not directly compromise DHRS availability, and whose annual frequency of occurrence (FAO) is taken to be equal to 1. Following the event, the reactor core is successfully shut down (i.e., the automatic reactor shutdown function is not modeled but supposed to function correctly), and the heat removal via the secondary sodium loop in-vessel heat exchangers (IHX) ceases. The primary pumps (PP) are supposed to continue to operate with a programmed coast-down after scram, characterized by a fixed halving time and fallback flow rate..

The reference duration of the mission ("mission time") is 1000 h. This duration was not selected based on actual safety studies but rather to amplify the influence of the dynamic aspects of the PRA, specifically the impact of repair and the physical model.

The benchmark proceeded in two phases:

I) Comparison of the implementations of the dynamic thermal-hydraulic model against the reference model MODENA using defined test cases. This phase, comprising test cases 1 to 4, is described in [1].

II) Comparison of the results of static and dynamic models and cross-comparison of the different dynamic approaches.

The comparative study of different dynamic approaches follows a multi-stage process, beginning with a comparison to the static model and subsequently analyzing differences between dynamic models. By comparing dynamic and static model results, we verify that dynamic models generate identical failure sequences (given identical success criteria and system mission times) and produce failure rates comparable to the static model under no-repair conditions. Two calculations are performed: one excluding and another including common cause failures (CCFs). A third calculation takes the possibility of repairs into account, and is therefore not compared with the static model, in order to see the influence of repairs. The resulting test matrix is represented in Table 1.

Table 1: Test matrix of the dynamic PRA benchmark

Test case	Types of calculation	CCF	Repair
Case 5	Static / Dynamic	No	No
Case 6	Static / Dynamic	Yes	No
Case 7	Dynamic	Yes	Yes

4.2. Benchmark results

The results of Case 5, comparing DHRS failure probabilities without CCF and repair considerations, are summarized in Table 2. The comparison validates the accurate modeling of event and failure trees for static calculations, and the simultaneous evaluation of the temperature criterion's impact within dynamic calculations. Applying the latter criterion reduces DHRS failure probability by approximately 25% over the 1000-hour mission.

Table 2: Comparison of calculation results for test case 5 (without CCF, without repair)

	Static calculation (min. requirement criterion) ***DHRS failure probability P_{s5}***	**Dynamic calculation (temperature criterion)** ***DHRS failure probability P_{d5}***	**Dyn./static ratio** ***P_{d5} / P_{s5}***
JPN calculation	1.3 E^{-5}	9.5 E^{-6} ± 2%	0.75
FRN calculation	1.2 E^{-5}	9.4 E^{-6} ± 0.4%	0.76

Table 3 presents the results of the calculations incorporating common cause failures (Case 6). The agreement between calculated probabilities confirms the accurate modeling of common cause failure effects.

Table 3: Comparison of calculation results for test case 6 (with CCF, without repair)

	Static calculation (min. requirement criterion) ***DHRS failure probability P_{s6}***	**Dynamic calculation (temperature criterion)** ***DHRS failure probability P_{d6}***	**Dyn./static ratio** ***P_{d6} / P_{s6}***
JPN calculation	3.9 E^{-5}	1.9 E^{-5} ± 2%	0.49
FRN calculation	3.8 E^{-5}	2.1 E^{-5} ± 0.4%	0.55

The comprehensive dynamic PRA analysis, incorporating common-cause failures (CCF) and the repair option, as presented in Table 4, demonstrates strong agreement between the two approaches. The repair option reduces the failure probability by 25% to 34%. Compared to the corresponding static calculation (P_{s6}), the dynamic approach yields a roughly 64% reduction in failure probability. A detailed analysis of the failed sequences with the JPN code reveals that they are dominated by irreparable component failures, thus limiting the effectiveness of the repair option.

Table 4: Comparison of calculation results for test case 7 (with CCF and repair)

	Dynamic calculation (temperature criterion) ***DHRS failure probability P_d***	**Ratio with case 6** ***P_{d7} / P_{d6}***
JPN calculation	1.4 E^{-5} ± 3.9%	0.75
FRN calculation	1.4 E^{-5} ± 0.1%	0.66

The excellent agreement between the JPN and FRN results instills confidence in the suitability of both methods. The incremental approach of the test matrix, designed to test key elements of modeling and probabilistic evaluation without possible compensation effects, allows for identifying the magnitudes of the different contributions of the DPRA approach. While the significant contribution of the temperature criterion is clearly demonstrated, the benefits of the repair option are largely obscured by the model's assumption of limited repairability for critical DHRS components.

5. CONCLUSION AND OUTLOOK

Evaluating the reliability of the decay heat removal system in sodium-cooled fast reactors is a compelling application for dynamic probabilistic risk assessment methods. These systems possess the unique characteristics of having a substantial grace period due to the high thermal inertia of the primary circuit, and long mission times, which allow for the possibility of repairing failed equipment during the mission. Accounting for these factors can reduce the conservatism inherent in static PRA approaches.

This study compares two numerical DPRA approaches developed in Japan and France, applied to a simplified DHRS model for the ASTRID reactor. Following the validation of the physical model in the first part of this study [1], the results presented here show excellent agreement between the two approaches for all analyzed scenarios, including those involving repairs of failed components. The results also quantitatively demonstrate the benefits of applying a success criterion based on the physical model and considering repair possibilities.

The Japanese PRIME method has the advantage of identifying dominant failure sequences, which might be used to optimize DHRSs and their subsystems. The French DayDREAM method, while unable to identify the most significant contributing minimum cut sets (MCS) to failure risk, excels in its ability to rapidly simulate sequences, making it particularly valuable during the design phase for parametric studies, such as those involving mean repair times.

This benchmarking exercise will be complemented by a sensitivity study on the mission duration and the performance of the S2 system , as well as by propagating the uncertainties of the input parameters through the models in order to demonstrate the methods' robustness.

Acknowledgements

The lead author would like to thank JAEA, MHI, MFBR and MHINSE for the continued support in this study. Some analyses in the benchmark have been performed using the RiskSpectrum PSA being developed by RiskSpectrum AB. The paper includes some of the results of the “Technical development program on a common base for fast reactors” and "Technical development program on a fast reactor for demonstration" ensured to JAEA by the Ministry of Economy, Trade and Industry in Japan (METI).

References

[1] Ihara, Koki, et al. “Benchmark on dynamic PRA with simplified decay heat removal system model of sodium fast reactor – Part 1 (Benchmark analysis condition and thermodynamic model results)”, PSAM17/ASRAMS2024, to be published

[2] Gauché, François, et al. “The French Fast Reactor Program – Innovations in Support to Higher Standards”, FR13 Paper IAEA-CN-199-INV-062, 2013

[3] Lloyd's Register Consulting - Energy AB, “RiskSpectrum Analysis Tools”, Theory Manual, Version 3.3.0, Lloyd's Register Consulting - Energy AB, 2016

[4] Aubert, Florence, et al. "Implementation of probabilistic assessments to support the ASTRID decay heat removal systems design process." Nuclear Engineering and Design 340 (2018): 405-413.

[5] Eide, Steven A., et al. “Generic, Component Failure Data Base for Light Water and Liquid Sodium Reactor PRAs”. No. EGG-SSRE-8875. Idaho National Lab.(INL), Idaho Falls, ID (United States), 1990.

[6] Ma, Zhegang, et al. “Industry-Average Performance for Components and Initiating Events at US Commercial Nuclear Power Plants: 2020 Update”. No. INL/EXT-21-65055-Rev000. Idaho National Lab.(INL), Idaho Falls, ID (United States), 2021.

[7] Gauthé, Paul, et al. “Level-1 PSA Studies for the ASTRID Reactor”. In: Proc. Int. Conf.PSA 2013, Columbia, South Carolina, USA.