Reliability Estimation Method for SMR Passive Safety Systems

Tero Tyrväinen[a], Essi Immonen[b], and Atte Helminen[b]
[a] Steady Energy, Espoo, Finland, tero.tyrvainen@steadyenergy.fi
[b] VTT Technical Research Centre of Finland, Espoo, Finland, firstname.surname@vtt.fi

Abstract: Passive safety systems are incorporated extensively in current SMR designs. Compared to active safety systems, which are driven by external power sources, and must be activated to function, passive safety systems rely more on physical phenomena, like gravity or natural circulation. Because of the nature of the phenomena, such as weak driving forces in natural circulation, the assessment of the failure probability for a passive function is challenging.

The paper presents a reliability estimation method of passive safety systems in order to support the probabilistic risk assessment (PRA) of small modular reactors (SMR). The method has been influenced by the guidelines of EPRI and IAEA, and it can be summarized in two main consecutive steps. First, the scenarios that induce different conditions to the passive safety system are systematically and thoroughly identified, grouped and screened. Second, the conditional failure probability of the passive safety function is estimated using expert judgment in each scenario. Thermal-hydraulic simulations are used to support the expert judgments.

Compared to many existing methods, which are often simulation-based, this method avoids the performance of a very large number of deterministic simulations. In the method, the integration of plant level scenarios and conditions to component level phenomena and estimating their impact to system level reliability supports the very needs of PRA. The method is demonstrated in the paper using the LDR lite SMR design concept, which is a public research study version of the LDR-50 SMR design created at VTT and now developed and commercialized by Steady Energy. The LDR lite design, which is a low-temperature, integral, district heating reactor, relies on passive emergency core cooling function that is in the focus of the presented reliability analysis demonstration.

1. INTRODUCTION

Passive safety systems are present in many current SMR designs. For the passive systems, in comparison to active systems, the reliability assessment needs to be extended from analyzing mechanical component failures to also analyzing the degradations and failures of the physical phenomena that the system relies on, such as gravity or natural circulation.

There are multiple existing reliability analysis methods that typically rely on thermal-hydraulic (T-H) simulations of passive systems using best-estimate codes [1]. The most common approach is to define uncertainty distributions for the input parameters of the T-H model, propagate the uncertainties through the T-H model for example using Monte Carlo simulations and estimate the failure probability of the passive system based on how often a failure domain was reached in the simulations.

Methods that emphasize the integration of the reliability analysis of the passive system with the probabilistic risk assessment (PRA) are not widely found in literature. Guidelines of EPRI [2] and IAEA [3] provide useful support for identification of analysis scenarios. EPRI [2] recommends a practical expert judgment -based approach for the quantification. With influence from those guidelines, this paper develops a comprehensive expert judgment -based reliability assessment method for passive systems to support the PRA of SMRs.

2. PROBLEMS WITH THE UNCERTAINTY PROPAGATION APPROACHES

For the quantification of phenomenological failures, an expert judgment -based approach is selected in this paper, whereas uncertainty propagation methods have often been proposed. Uncertainty propagation is not selected here due to the following reasons:

- Uncertainty propagation requires a large number of time-consuming simulations.
- Uncertainty propagation works well mainly if the safety function fails in some of the simulations. If the safety function does not fail, the simulations produce quite little information compared to the computation time (though they obviously give good evidence on the reliability of the passive system). In such a case, there is a possibility to estimate a probability distribution for a critical parameter, such as core temperature, based on the simulation results and use that distribution to estimate the probability that the "failure threshold" is exceeded (as applied e.g. in [4]). However, it is highly questionable if the probability distribution can really be estimated properly from the simulation results, particularly the tail of the distribution that is the most important part.
- Uncertainty propagation also requires expert judgments concerning the probability distributions of the input parameters.
- The uncertainty propagation concentrating purely on the input parameters does not take into account uncertainty related to the simulation model/software, and therefore, does not treat sufficiently the modelling related uncertainties.
- Time-consuming uncertainty propagation needs to be repeated when the simulation model is updated.
- PRA analysis can involve many accident sequences that require separate assessment of the passive system reliability. This increases the workload and the number of required simulations further.

3. RELIABILITY ANALYSIS METHOD FOR PASSIVE SYSTEMS

This section presents a method for the reliability analysis of passive systems to support the PRA of SMRs. The main features of the method are to

- identify comprehensively different scenarios where the conditions in the passive system are different;
- estimate the reliability of the passive system in each identified scenario in a practical way without an extensive number of deterministic simulations.

The method includes the following main analysis steps:

1. Characterization of the system
2. Identification of events and deviations
3. Identification and selection of accident scenarios
4. Quantification of mechanical component failures
5. Quantification of phenomenological failures

The analysis steps are briefly described in the following subsections.

3.1. Characterization of the System

The general information of the system is defined, including the operating principle of the system and the components that belong to the system, the mission and success criteria of the system, and interfaces with other systems. Also, the boundaries of the analysis, such as plant operating states, are defined.

3.2. Identification of Events and Deviations

The events that can change conditions in the passive system are identified, and the consequences of the events on the passive system are evaluated qualitatively. Both failure modes and effects analysis (FMEA) and hazard and operability study (HAZOP) are used in the identification.

FMEA is developed for each component of the passive system as well as for relevant components of the connected systems. The consequences of failures are considered from the passive safety function's point of view.

In HAZOP, deviations in the parameters influencing the physical phenomena of the passive system are analysed. The first step is to identify the physical phenomena that are relevant to the operation of the system (meaning that the safety function could fail if the phenomena do not occur as expected). The second step is to identify the parameters that can influence those phenomena. The third step is to identify possible causes and consequences for deviations in each identified parameter. The consequences are considered from the passive safety function's point of view.

3.3. Identification and Selection of Accident Scenarios

This step includes the following substeps:

a. The initiating events relevant to the analysis are identified and grouped based on the conditions they induce on the passive system and consequent accident progression. The FMEA, HAZOP and initiating events of the PRA model are utilized in this process.
b. For each initiating event group, additional failures/events that can occur after the initiating event and affect the passive system are identified based on the FMEA, HAZOP and PRA model.
c. Scenarios for the analysis are identified by combining the IE groups with the additional failures/events. There will be scenarios with only an initiating event, an initiating event and one additional failure, an initiating event and two additional failures, etc.

3.4. Quantification of Mechanical Component Failures

Frequencies for the previously identified scenarios are estimated using normal PRA techniques. The PRA model can be utilized in this. Scenarios with very low frequency are screened out.

3.5. Quantification of Phenomenological Failures

The conditional failure probability of the passive system is estimated in each scenario by expert judgment supported by information from the FMEA, HAZOP, deterministic simulations and experiments if available. EPRI has provided good guidelines [2] for making expert judgments and utilizing simulations.

Deterministic simulations to support expert judgments should mainly focus on scenarios that involve uncertainty. There is no need to perform simulations if the result is known beforehand, i.e. the safety function's failure probability is clearly 1 or 0. In uncertain cases, it is likely best to perform simulations iteratively, i.e. perform one simulation and think what kind of variations would provide additional information. The simulations should particularly focus on finding conditions (parameter values) where the safety function fails or is degraded. EPRI's approach [2] of dividing the scenario into sub-scenarios with regard to the values of input parameters in the quantification can be followed if seen beneficial.

4. APPLICATION TO EXAMPLE CASE

The reliability analysis method is demonstrated with an example case, the passive core cooling system (PCCS) of the LDR lite. The scope of the analysis is narrowed to power operation of the reactor and to internal initiating events. The whole analysis is not presented, but representative parts to demonstrate the analysis method in practice. Step 4, quantification of mechanical failures, is omitted, as at the time of the analysis, a full PRA model was not available. Also, the analysis relies heavily on expert judgments as it was not possible to perform many deterministic simulations to support this preliminary analysis.

The LDR lite design is described in detail in a public benchmark description [5]. The LDR lite module is illustrated in Figure 1. The reactor vessel contains the whole primary circuit, and is nested inside the containment vessel, which is submerged in the pool. The primary coolant flow is driven by natural convection. The reactor is pre-pressurized with a nitrogen bubble at the top of the reactor. Heat is transferred to the district heating network through a secondary circuit and two sets of heat exchangers.

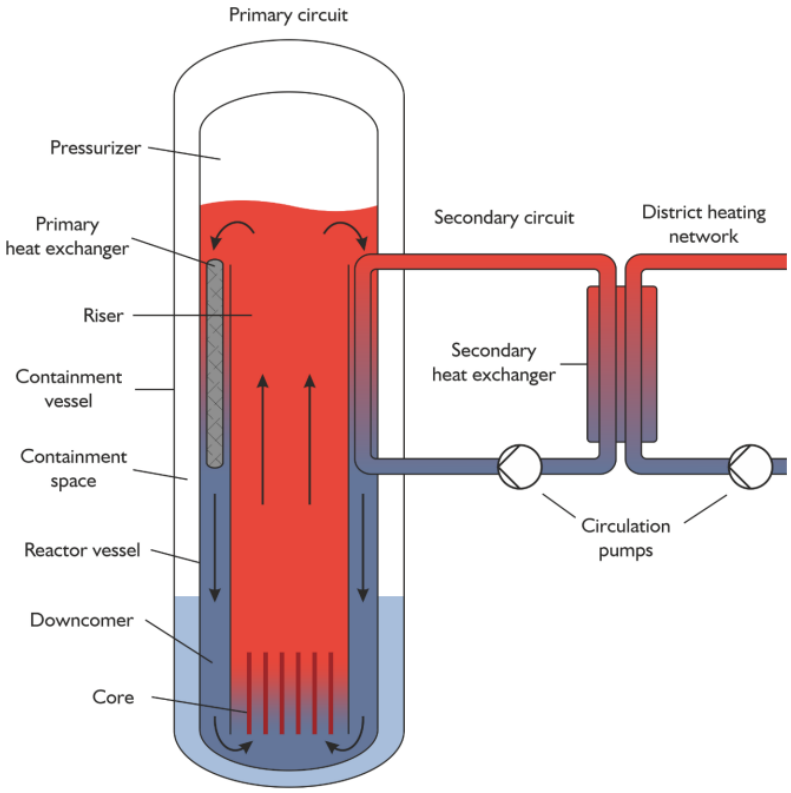

Figure 1: A schematic of the LDR lite module. [5]

4.1 Characterization of the System

During accidents, if the cooling through the secondary circuit is either lost or disconnected, the heat is transferred from the reactor to the pool through the PCCS. The downcomer temperature starts to increase and the heat transfer through the containment is enhanced. The PCCS consists of the reactor vessel (RV) and its water inventory, the containment vessel (CV) and its water inventory, and the reactor pool (RP). Heat is transferred from the reactor core to the sides of the RV (containing the primary heat exchangers that are used during normal operation) by natural circulation in the reactor coolant system. Without active cooling, heat is conducted through the RV wall to the water and gas volume in the CV. The water in the CV will start to evaporate causing steam to condense on the inner surface of the CV. This enables efficient heat transfer from the CV to the RP.

The RV has two sections, the head and the vessel body. In the upper part of the vessel body, there are welded nozzles for the inlets and outlets of the heat exchangers and the chemical and volume control system (CVCS) make-up and let-down. The vessel head has penetrations for overpressure protection and instrumentation.

The CV is the outer surface of the reactor module and acts as the outermost release barrier. The space between the CV and the RV is partially filled with water to provide the passive cooling function. The CV has two parts, the vessel head and the vessel body. There are several nozzles and penetrations for secondary system and CVCS lines in the vessel body and also in the head for the overpressure protection and instrumentation.

The pool is made of concrete with a 5 mm stainless steel plate lining. The pool dimensions are approximately 8.5 m x 8.5 m with 15 m depth. The pool is filled with water that is kept at 30 degrees Celsius.

The mission of the PCCS is to transfer heat from the reactor core to the RP. The safety function is considered successful if core damage is avoided.

The PCCS has the following interfacing systems:

- primary heat exchangers
- reactor core
- control rod system
- secondary system
- chemical and volume control system
- overpressure protection valve in RV
- overpressure protection valve in CV

The analysis is limited to power operation states.

4.2 Identification of Events and Deviations

FMEA was performed for the components of the PCCS and also any relevant interfacing system components. In some cases, failure modes of a system were considered on system level. For each failure mode, the possible causes and consequences from the viewpoint of the PCCS were identified. Finally, the PCCS performance in each failure mode was tentatively assessed by expert judgment, e.g. whether the system is operable, degraded or failed. Part of the FMEA is presented in Table 1.

Table 1: FMEA for selected components

Component	Failure mode	Cause	Consequence	PCCS performance
Main heat exchanger (inc. tube, shell, gasket)	Leak / rupture	Overpressure in secondary side, manufacturing defect, maintenance error, dropping during maintenance, ageing effects, gasket failure, failure in attachment mechanism, bolts left untightened	Leak from the secondary system to the RV. The reactor coolant system is extended to the secondary system isolation valve. The pressure of the RV increases.	Fully operable.
Containment vessel	Leak	Manufacturing defect, ageing, corrosion, gasket failure	Depending on the size of the leak and CV pressure, RP water may leak inside or gas from the CV may leak to the RP.	Fully operable, failure possible if water from CV is lost.

Containment vessel	Rupture	Manufacturing defect, ageing, corrosion, gasket failure	RP water leaks inside. The water volumes of the CV and RP become directly connected. This increases heat transfer.	Fully operable.
Reactor vessel	Leak	Manufacturing defect, ageing, corrosion, gasket failure, RV overpressure protection valve spurious opening	Water leaks from the RV to the CV. The water level and pressure in the CV increase. The water level and pressure in the RV decrease. Heat transfer increases.	Fully operable.
Reactor vessel	Rupture	Manufacturing defect, ageing, corrosion, gasket failure	Water leaks from the RV to the CV. The water level and pressure in the CV increase. The water level and pressure in the RV decrease. The natural circulation inside the RV is lost, because the water level is decreased below the riser barrel. The water volumes of the RV and CV become connected. Heat transfer increases.	Fully operable.
Secondary system line inside the containment vessel	Leak / rupture	Manufacturing failure, ageing, welding defect, seismic event, failure in the support of the RV	The pressure and water level inside the CV increase. Heat transfer from the CV water is increased, but heat transfer from the gas space is decreased. After the initial phase, the total heat transfer should increase.	Fully operable.
CVCS make-up line	Loss or decrease of flow	Pump failure, valve failure, leak	The water level inside the RV starts to decrease. The decrease stops when the let-down line is isolated or the water level decreases to the level of the let-down line. The operation of the decay heat removal could be degraded (natural circulation through the downcomer lost) if the water level decreases below the riser barrel top elevation.	Fully operable, degraded in the worst case.
CVCS line outside the containment vessel	Leak / rupture	Manufacturing failure, ageing, welding defect, seismic event	If the isolation valves fail, the RV water starts to boil and the water level decreases slowly. The operation of the PCCS could be degraded (natural circulation through the downcomer lost) if the water level decreases below the riser barrel top elevation. In long term, core uncovery occurs.	Degraded or failed if isolation fails
Reactor pool	Leak	Tool falling, earthquake	If the CV is under water, the PCCS works. Otherwise, the PCCS can be assumed failed.	Failed if CV is uncovered.

As part of HAZOP, the following physical phenomena related to the PCCS operation were identified by expert judgment:

- Evaporation of the water inside the CV

- Steam condensing on the inner surface of the CV
- Natural circulation inside the RV
- Natural circulation (both liquid and gas) inside the CV
- Natural circulation inside the RP

There are parameters that influence each of the identified phenomena. For evaporation inside the CV, condensing on the inner surface of the CV and natural circulation inside the CV, the parameters are the following:

- Pressure inside the CV
- Water temperature inside the CV
- Temperature at the inner surface of the RV
- Heat transfer coefficient of the RV
- Temperature at outer surface of the CV
- Heat transfer coefficient of the CV
- Inter-vessel pool water level
- RP water level
- RV water level
- Nitrogen concentration inside the CV
- Composition of non-condensable gases inside the CV
- Temperature of the penetrating hot and cold leg pipes

The parameters affecting natural circulation inside the RV are:

- Flow rate inside the RV
- Reactor power
- RV wall heat transfer distribution
- Flow resistance of the circulation flow inside the RV
- RV water level

The parameters affecting natural circulation inside the RP are:

- CV wall heat transfer distribution
- Temperature distribution of the RP
- RP water level
- Flow rate inside the RP

A HAZOP analysis was conducted as part of the full assessment, but in this specific case it did not provide any additional events of significance compared to the FMEA that was performed simultaneously. Thus, the HAZOP is not described further.

4.3 Identification and Selection of Accident Scenarios

To identify the relevant accident scenarios affecting the performance of the passive system, the FMEA was used to create initiating event groups. The initiating event groups were then combined with 0, 1 or 2 additional failures that could affect the performance of passive heat removal system. The secondary circuit was assumed failed or isolated in every scenario. Some events that were not considered to be significant for the passive heat removal could directly be omitted. Some representative scenarios are listed in Table 2. The estimation of the conditional failure probability in the third column of the table is discussed in the next section.

Table 2: Scenarios

Scenario	Description	Conditional failure probability
General transient	An initiating event that has no impact on the PCCS occurs, and the reactor trip is performed.	1E-7
Leak at the bottom of the CV	There is a leak at the bottom of the CV. The reactor trip is performed.	0.01
Leak from the RV to the CV and CV leak	There is a leak from the RV to the CV. There is also a leak in the CV. The reactor trip is performed. There is no make-up for the RV water.	1
CVCS LOCA and failure to isolate	There is a leak in the CVCS with a direct path from the RV to outside the system boundary. Isolation fails. The reactor trip is performed. There is no make-up for the RV water.	1
Loss of CVCS make-up and failure to isolate CVCS	CVCS failures decrease the RV water level below the elevation of the riser barrel. The reactor trip is performed.	1E-4

4.4 Quantification of Phenomenological Failures

The quantification for this example case focuses on the phenomenological failures. For full analysis, the mechanical failures should be assessed simultaneously.

The conditional failure probability of the PCCS in each of the scenarios was estimated by expert judgment. For the estimation, supporting information was collected from the FMEA conclusions, HAZOP and simulations that had been already performed for the scenario (in most cases, there were no simulations). Based on the information, the performance of the system and uncertainty were qualitatively assessed, and the conditional failure probability was chosen from the categories of Table 3. The results for selected scenarios are presented in Table 2.

Table 3: Failure probability estimates

Qualitative assessment	Conditional failure probability
The PCCS cannot fail in this scenario	1E-7
The PCCS should not fail in this scenario, but there is some uncertainty	1E-4
The PCCS could possibly fail, but it is unlikely	0.01 or 0.1
The PCCS is assumed to fail	1

Similar approach to the categorization of the failure probability estimates is described in [2]. For many scenarios, the qualitative assessment was that the passive heat removal cannot fail. For those cases a failure probability above 0 was selected to cover possible unidentified failure mechanisms. The value

1E-7 has been used in literature for similar systems, such as NuScale's emergency core cooling system [6].

It can be concluded that, in practice, the PCCS fails only if enough water is lost either from the RV, CV or RP. Otherwise, the PCCS is expected to function.

5. DISCUSSION

The reliability analysis of a passive system should be an iterative process. For passive systems in SMRs, tentative reliability estimates are needed already in the conceptual design phase. During the design process, the knowledge on the passive system performance increases through simulations and experiments, and the reliability estimates can then be updated. The PRA combined with passive system reliability analysis can support the selection of the thermal-hydraulic simulations to reduce uncertainties in risk-significant scenarios. The method presented in this paper supports this kind of iterative analysis process and a graded approach.

For PRA, uncertainty distributions for the probability estimates need to be estimated, although it is a challenging task solely relying on expert judgment. Further effort should also be put to studying the different types of uncertainties present, e.g. epistemic and aleatory. The uncertainty distribution of the failure probability should represent epistemic uncertainty, whereas the failure probability itself represents aleatory uncertainty on the occurrence of a failure. Obviously, the epistemic uncertainty related to the estimates is large, but the role of aleatory uncertainties is more unclear at this point.

The strength of this type of passive system reliability analysis approach is the clear connection to the PRA model. The level of detail of making estimations to multiple separate scenarios gives flexibility to the PRA analyst in comparison to some more deterministic uncertainty propagation methods. The method can also be used for preliminary assessment when there are not many deterministic simulations available, e.g. in conceptual design phase.

In future, the method could be improved by better definition of the process of collecting expert judgments. Also, the use of simulations in an efficient and practical way could be studied and instructed in more detail.

6. CONCLUSION

This paper introduces a comprehensive expert judgment -based reliability analysis method for passive systems and demonstrates the method for a SMR passive core cooling system. Main features of the developed method are comprehensive identification of possible accident scenarios affecting the passive system, and efficient use of expert judgment and simulations to quantify the phenomenological failures of the passive system.

The method presented supports the iterative safety analysis process in SMR conceptual design phase and is easily integrable into simultaneous PRA model development process.

Acknowledgements

The method development was started as part of the development work of LDR-50 with Steady Energy's funding and continued in the SAFER2028 research program. The authors thank the experts from VTT and Steady Energy for support with the analysis: Seppo Hillberg, Rebekka Komu, Ville Hovi, Daniel Lopez-Sole and Jaakko Leppänen.

References

[1] S. A. Olatubosun and C. Smidts. "*Reliability analysis of passive systems: An overview, status and research expectations*", Progress in Nuclear Energy, 143, 104057, (2022).

[2] Electric Power Research Institute. "*Program on technology innovation: Comprehensive risk assessment requirements for passive systems*", 2008, Palo Alto, California.

[3] International Atomic Energy Agency. "*Progress in methodologies for the assessment of passive safety system reliability in advanced reactors*", IAEA-TECDOC-1752, 2014, Vienna.

[4] 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, 53, pp. 498-508, (2021).

[5] R. Komu, R. Tuominen and V. Valtavirta. 2025. "*LDR lite benchmark specification."* LDR design document LDR-PUB-VTT-10002-R4, VTT Technical Research Centre of Finland, Available: https://serpent.vtt.fi/kraken/index.php?title=LDR_lite_benchmark .

[6] NuScale Power LLC. *"NuScale standard plant design certification application, Chapter nineteen: Probabilistic risk assessment and severe accident evaluation."* Revision 5: Part 2 – Tier 2, 2020.