Allocating Reliability Goals for SMR Passive Safety Systems

Atte Helminen and Essi Immonen
VTT Technical Research Centre of Finland, Espoo, Finland, forename.surname@vtt.fi

Abstract: As the nuclear regulatory framework and licensing requirements transition from prescriptive to more goal-oriented requirements, it is important to develop best practices for the setting of the reliability goals. This is especially important for small modular reactors (SMR), where the simplified safety design and use of passive systems impose high expectations for the reliability of the systems.

This paper describes a probabilistic risk assessment (PRA) model developed for the LDR lite SMR design concept. LDR lite is a public research study version of the LDR-50 SMR design. The PRA model is applied to define and allocate reliability goals to individual LDR lite systems. The influence of initial and boundary assumptions, such as risk criteria specific to different Defence-in-Depth (DiD) levels, on the goal setting is studied. Allocation of reliability goals based on PRA modelling provides sufficient flexibility to examine the possible impact of different assumptions. This flexibility has high importance when studying the reliability of SMR passive systems and determining if the reliability estimation method measures up to the allocated reliability goals.

The analysis method applied in the reliability estimation of the passive systems needs to be in line with the strictness of the reliability goals. For safety systems with lower reliability goals, the use of generic estimation methods and non-specific evidence for systems can be justified. For safety systems with higher reliability goals, such as a passive system responsible for a significant part of DiD protection of a plant, the reliability analysis methods need to be more sophisticated and developed for the application purpose, using case-specific evidence. It would be also beneficial if a graded approach can be applied in the method, as then the level of detail in the analysis can be set proportional to the reliability goals allocated for the passive systems.

1. INTRODUCTION

The simplified design and extensive use of passive systems in the safety design of small modular reactors (SMR) impose high expectations for the reliability of passive systems. Passive systems offer certain advantages over electric-driven, active systems. These advantages include for example the reduction of human interaction and the avoidance of external electrical power or signals. Passive systems are particularly convenient for scenarios involving loss or reduction of heat removal, where the passive systems can be used to perform key safety functions such as gravity-based safety injections or residual heat removal based on natural circulation.

Reliability estimation is more challenging for passive systems than active ones. The natural forces that drive the operation of passive systems are normally small and the counter-forces and other adverse effects can be of comparable magnitude. In the reliability estimation of active systems, the uncertainties involved in natural driving forces bear no meaning. The failure modes of active systems are typically component-related and the system reliability can be derived from the reliability of its components. For passive systems, the situation is more complex. The failure modes of passive systems are more phenomenological in their character and often depend on dynamic physical processes rather than discrete component failures. For a residual heat removal passive system, the failure modes can be, for example, weakened natural circulation due to pressure losses caused by degraded heat transfer or by non-condensable gases.

The increasing safety significance of passive systems emphasizes the need for effective reliability demonstration methods. Passive systems in SMR are almost without exception unique in design, and therefore their operational experience is sparse or non-existing. The reliability data for estimation is typically generated from experimental testing or thermal-hydraulic simulations, both of which are either expensive or time-consuming to perform.

Over time several reliability estimation methods of passive systems have been developed. A recent overview of different methods can be found in [1]. Since the failure of a passive system depends strongly on the plant conditions, the system reliability can also be different in different plant conditions. For a non-trivial passive system, the uncertainties created by different plant conditions can easily explode the amount of analysis work required in the reliability estimation. To manage the workload, it would be beneficial to have a graded approach to support the reliability estimation so that more detailed analysis is performed in situations where the reliability of the passive system has a greater impact on plant safety.

This paper describes a probabilistic risk assessment (PRA) model developed for the LDR lite SMR design concept. The model presents a generic transient challenging the residual heat removal of the plant. The PRA model is used to define and allocate reliability goals to a passive system taking care of the decay heat removal through the containment. The risk metrics and estimates provided by the PRA model are used to evaluate if the allocated reliability goals for the passive system are sufficient from plant safety point of view. On the other hand, the calculated risk metrics and estimates can be used to evaluate if the analysis method and efforts applied to the reliability estimation of certain event and plant condition are in line with the strictness of the reliability goals assigned to the passive system.

The aim of this study is to demonstrate the idea of supporting the reliability estimation of passive systems with the reliability goal definition and allocation by PRA. The PRA model and the estimated values are only given as an example with no correspondence to a real PRA model.

2. OVERVIEW OF LDR LITE SMR

The LDR lite design specifications are presented in a public benchmark description. The public benchmark description is maintained by VTT and is publicly available on the internet [2]. In the LDR lite design, the reactor vessel contains the whole primary circuit. The reactor vessel is nested inside the containment vessel, which is submerged in a 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. The LDR lite design is described in more detail in the “Reliability estimation method for SMR passive safety systems” paper of PSAM-18 conference [3].

LDR lite is a public research study version of the LDR-50 SMR design. In LDR lite, many of the LDR-50 systems have been stripped-down or completely removed. The purpose of LDR lite design is to support the benchmarking activities of different research projects on SMR safety and applications. The specifications are currently applied in two EU-level research projects where the simulation and analysis abilities of different European organisations are benchmarked for SMR safety on electric [4] and non-electric applications [5].

Since the focus of LDR lite design specifications has been in the simulation benchmarking, the specifications leave open questions, for example, from the Defence-in-Depth viewpoint. To create more plausible plant design and to make the reliability allocation of safety systems more feasible, the LDR lite design specifications need to be expanded to include some relevant safety systems. Some of the additions benefit from the design descriptions outlined for an early reactor design version of LDR-50 in [6]. The additions to the LDR lite specifications are following:

- Addition of diverse reactivity control system with two boron injection systems (BIS). The systems inject the boron to the reactor vessel through two redundant chemical and volume control systems (CVCS), see the system configuration inside the dash line in Figure 1.
- Addition of shutdown cooling systems (SDCS) to two redundant secondary circuits, see the system configuration inside the dash line in Figure 2.

The additions make the LDR lite design specifications more realistic, and at the same time, ensure that the reliability goals allocated for the safety systems remain sensible.

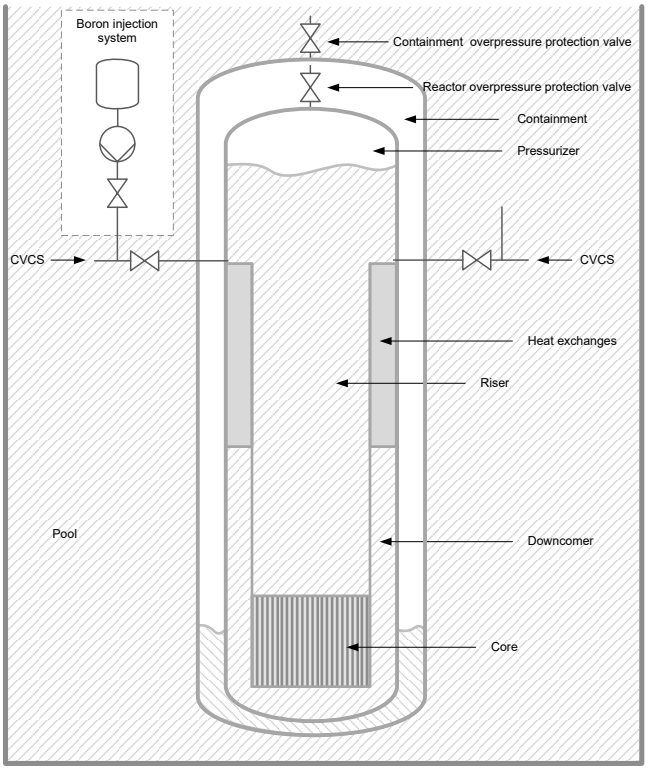

Figure 1: Addition of BIS to LDR lite design.

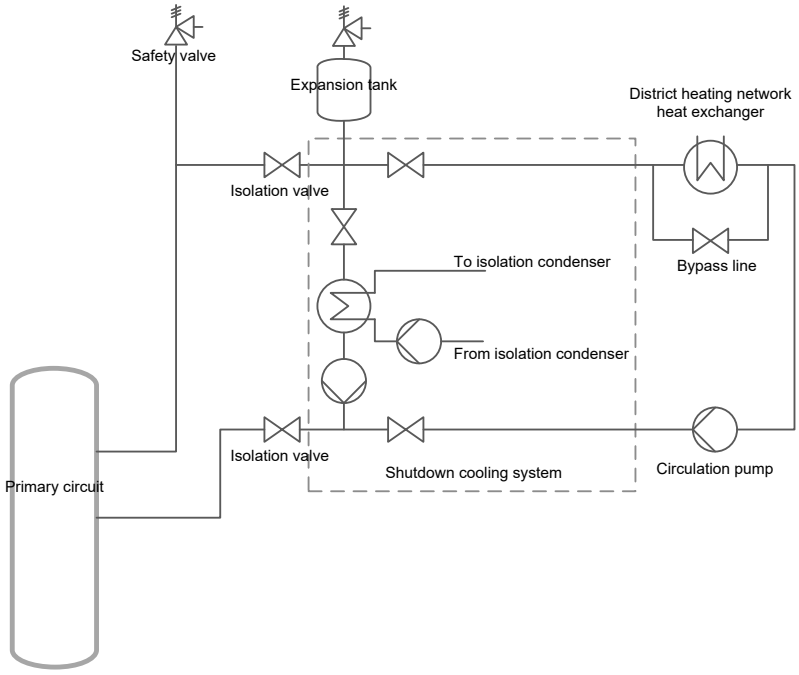

Figure 2: Addition of SDCS to LDR lite design.

3. PROBABILISTIC RISK CRITERIA AND RISK MODEL

Probabilistic criteria have been analyzed by the OECD NEA Working Group on Risk Assessment [7], and by the Nordic nuclear safety research organization [8]. The numerical criteria differ across countries in both formulation and regulatory status. In several countries, different numerical values are applied to existing and new nuclear power plants, with more stringent targets generally imposed on new designs. Figure 3 from [8] summarizes the numerical criteria defined for core damage frequency (CDF) criteria, typically expressed per reactor-year.

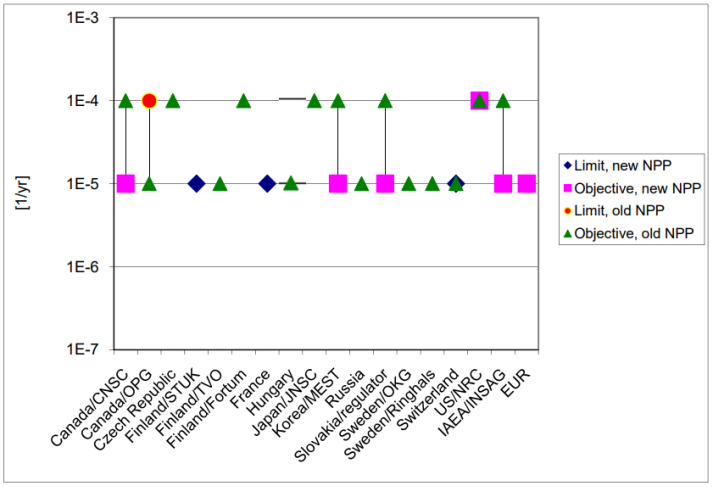

Figure 3: Core damage frequency criteria in different countries.

Typical target values for new plants are of the order of 10^{-5} per reactor-year, with less stringent values (e.g. 10^{-4} per reactor-year) applied to existing plants. The target value of 10^{-5} per reactor-year can be used as a starting point for this study.

To use the yearly CDF target value as such, a full PRA model should be created. This is not possible for LDR lite. The reliability goal allocation of this study is limited to the modelling and analysis of sequences of a single initiating event. There are no international standards on how to define numerical target values of CDF for single sequence or initiating event. For this study, it is assumed that the risk contribution of single (but quite frequent) initiating event should not exceed 1% of the yearly CDF criteria. This sets the CDF target value for the single event to 10^{-7} per reactor-year.

The probabilistic risk model consists of an event tree for the loss of district heating network transient. The systems and their success criteria (in parentheses) in the different sequences of the risk model are illustrated in the logical diagram in Figure 4. In normal operation, the heat produced by LDR lite is consumed by the district heating network. In case of failures in the heat exchangers of redundant parts of the district heating network (see upper right part of Figure 2), a reactor scram is actuated, and the residual heat is removed from the reactor.

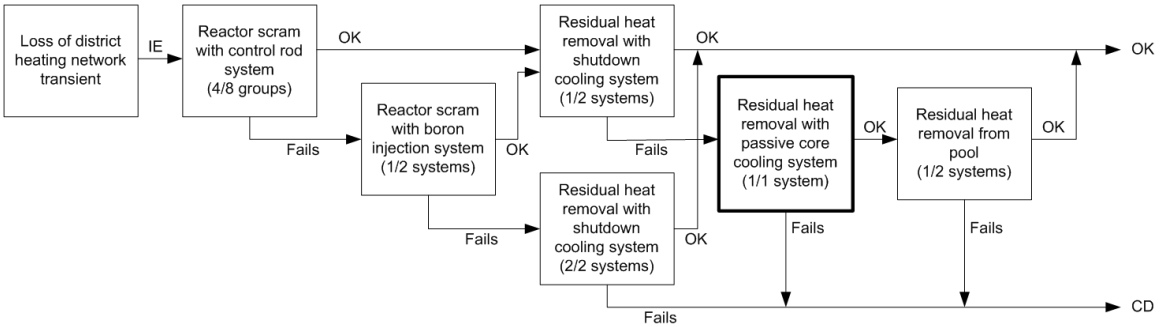

Figure 4: Logical diagram of the risk model.

The reactor scram can be performed by two diverse systems: Control rod system (CRS) and boron injection system (BIS). CRS is composed of 8 control rod groups. For the study, it is assumed that success of 4 out of 8 control rod groups is sufficient to bring the reactor to safe shutdown. BIS has two redundancies. For the study, it is assumed that success of 1 out of 2 systems is sufficient to bring the reactor to safe shutdown.

The residual heat can be removed from the reactor with two diverse systems: Active shutdown cooling system (SDCS) and passive core cooling system (PCCS). SDCS uses isolation condensers to conduct heat outside. PCCS conducts heat to the pool where the containment vessel is submerged. SDCS has two redundancies. For the study, it is assumed that success of 1 out of 2 SDCS systems or PCCS alone is sufficient for residual heat removal, if the reactor scram has been successful. If the reactor scram hasn't succeeded, the functioning of both SDCS systems or PCCS and at least one of the SDCS systems are necessary for the constant removal of heat produced by the reactor. For the heat removal with PCCS to function for a long period of time, the pool cooling needs to be ensured.

For the risk calculations, generic values for component unavailability have been applied. No supporting systems are included in the model. No common cause failures are assumed. The initiating event frequency is set to 5 times per year.

4. RELIABILITY GOAL SETTING FOR LDR LITE PASSIVE SYSTEM

The passive system of interest in this reliability allocation study is the PCCS. The continuously operating system conducts the residual heat passively from the reactor vessel through the containment to the pool. The functioning of PCCS is described in detail in [3]. The role of PCCS in the risk model is illustrated with the bold borderline box in Figure 4. The failure of PCCS has been modelled as a single basic event. The failure probability of the basic event is variated to see how the variation impacts the core damage frequency (CDF) and the PCCS share of CDF, i.e. PCCS Fussell-Vesely value.

The results for different failure probability values of PCCS ranging from $1 \cdot 10^{-3}$ to $1 \cdot 10^{-7}$ are presented in Table 1. The values of other basic events in the model are kept fixed. The approximate system level failure probabilities for the other safety systems are listed in Table 2. As an example, the calculated estimates for the consequences of different branches in the event tree are shown in Figure 5. The calculations have been carried out with FinPSA program [9].

Table 1: CDF and PCCS Fussell-Vesely values for different failure probabilities of PCCS.

PCCS failure probability	CDF (MCA)	PCCS Fussell-Vesely
1,00E-07	5,86E-08	0,004
1,00E-06	6,06E-08	0,037
1,00E-05	**8,08E-08**	**0,278**
1,00E-04	2,83E-07	0,793
1,00E-03	2,30E-06	0,975

Table 2: Approximate failure probabilities of other safety systems.

System/Event	Approximate failure probability
CRS-FAILURE	1,7E-05
BIS-FAILURE	6,2E-04
SDCS-FAILURE-BOTH	4,5E-04
SDCS-FAILURE-ANOTHER	4,2E-02
POOL-FAILURE	2,5E-05

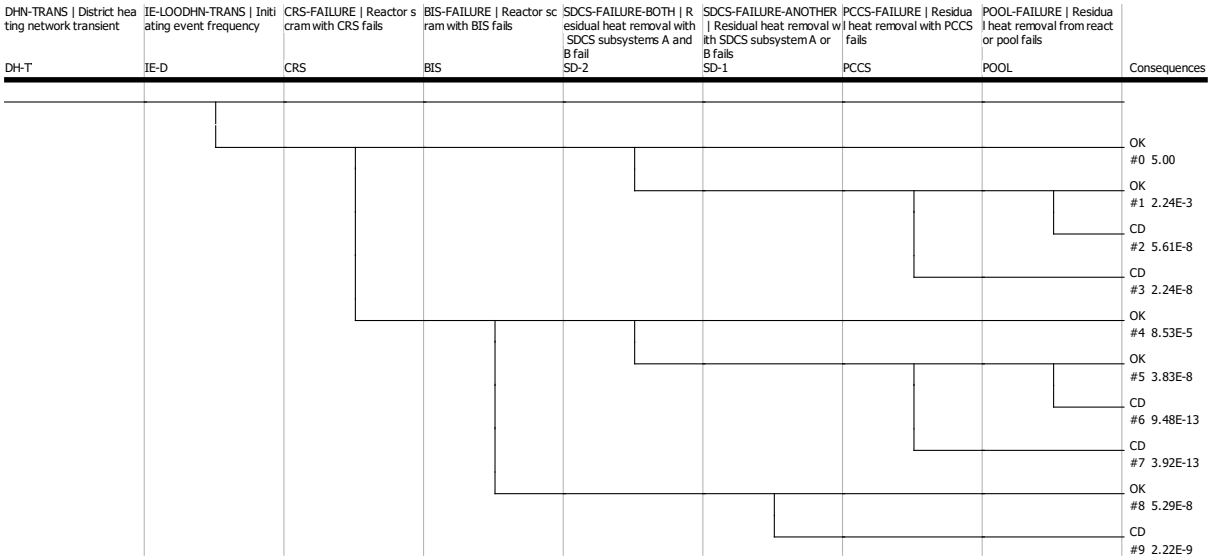

Figure 5: Calculated estimates for different branches of event tree ($P_{fail, PCCS} = 1 \cdot 10^{-5}$).

Based on the calculation results at least a reliability goal of 10^{-5} is required for PCCS in order to reach the CDF target value of 10^{-7} per reactor-year for the loss of district heating network transient. With this reliability goal, the PCCS contribution from the CDF is approximately 28%, so it is in balance with the risk significance of LDR lite safety systems involved in the transient.

5. DISCUSSION ON RELIABILITY GOAL SETTING FOR PASSIVE SYSTEMS

Based on the calculation results, it can be concluded that a sweet spot for the failure probability of PCCS would be somewhere in magnitude of 10^{-5}. With this reliability goal the CDF target value is reached (the numbers in bold in Table 1) and the risk contribution from the failure of PCCS doesn't stand out from the risk contributions of other safety systems involved in the transient. Naturally, the risk contribution of PCCS is bound to the failure probability of pool cooling system, since both systems are needed for the residual heat removal to operate through the pool.

The presented PRA model is not very realistic. The applied failure probabilities are general, and the model lacks the supporting systems and other system dependencies. The model, however, serves the purpose of the study. To create a comprehensive risk model of SMR all contributing safety systems should be included and reliability estimates for the systems, or their components, should be available. Therefore, it is easy to think that it is a one-way process where the reliability estimation serves the risk modelling. In the challenging reliability estimation of passive systems, it is better to consider the process as iterative, where the PRA model is created simultaneously providing feedback for the reliability estimation process.

In [3], a reliability estimation method for SMR passive systems is presented. The method is used to estimate conditional failure probabilities of a passive system in different scenarios. Expert judgments are applied extensively in the method. The main reason for the extensive use of expert judgements is to avoid the performance of large number of time-consuming deterministic simulations for the different scenarios. The lesser number of simulations may increase the uncertainties for the expert judgements. The uncertainties and their impact on plant safety should be considered when conducting the expert judgement process. Using PRA modelling for the setting of reliability goals for the SMR passive systems and evaluating their safety significance in different scenarios is a convenient way of providing feedback for the expert judgement process. This way the uncertainties can be reflected against their impact on plant safety. If the uncertainties have a high safety significance, it is worth consideration to run more simulations or collect other case-specific evidence on the reliability of the passive system.

For SMR, where a passive system has a big role in the Defence-in-Depth design of the plant safety, sophisticated reliability analysis methods and case-specific evidence should be applied. On the other hand, since the uncertainties created by different plant conditions can easily explode the amount of analysis work, it is beneficial to have a graded approach to support the reliability estimation so that more detailed analysis is invested for scenarios where the reliability of the passive system has a greater impact on plant safety. Defining and allocating reliability goals for SMR passive systems with PRA is a good practice to execute the graded approach.

6. CONCLUSION

The reliability estimation of SMR passive safety systems is a challenging task. The uncertainties created by different plant conditions can easily explode the amount of analysis work in the estimation. To manage the workload and to quantify the reliability estimates expert judgements are commonly applied. To support the expert judgement process, it is beneficial to use PRA modelling for the defining and allocating reliability goals for the SMR passive systems. With the PRA model and allocated reliability goals, it can be evaluated if certain plant level safety targets can be reached and if the risk significance of safety systems involved in different plant conditions are in balance.

Acknowledgements

The paper has been created in EASI-SMR and SANE projects co-funded by the European Commission and performed as part of Euratom Research and Training Programme, under contracts 101164810 (EASI-SMR) and 101163929 (SANE).

References

[1] Y. Louet, F. Mascari, E. Cilia, B. Grosjean, O. Sevbo, J. C. De La Rosa BluL, O. Zhabin, D. Grishchenko and P. Bízek. *"Identify and review the methodologies currently used for passive system reliability evaluation"*, Deliverable D4.1 of EU-EASI-SMR project, 2025. Available: https://easi-smr.eu/docs/resources/D4.1-Identify-and-review-the-methodologies-currently-used-for-passive-system-reliability-evaluation.pdf

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

[3] T. Tyrväinen, E. Immonen and A. Helminen. *"Reliability estimation method for SMR passive safety systems"*, Probabilistic Safety Assessment and Management Conference, PSAM-18, Pittsburgh, United States, 2026.

[4] https://easi-smr.eu/

[5] https://www.sane-euratom.eu/

[6] R. Komu, T.J. Lindroos, S. Hillberg, and J. Leppänen. *"District heating reactor LDR-50: Thermal-hydraulic analysis of difficult load following cases"*, The 13th International Topical Meeting on Nuclear Reactor Thermal-Hydraulics, Operation and Safety (NUTHOS 13), Hsinchu, Taiwan, 2022.

[7] OECD/NEA. "*NEA/CSNI/R(2009)16, Probabilistic Risk Criteria and Safety Goals",* OECD Publishing, Paris, 2009.

[8] J.-E. Holmberg and M. Knochenhauer. "*NKS-227, Guidance for the definition and application of probabilistic safety criteria"*, NKS Secretariat, Roskilde, Denmark, 2011.

[9] https://www.vttresearch.com/en/knowledge-base/finpsa-software-risk-informed-decisions-nuclear-plants