# Small Modular Reactor Multi-Module PSA

M. OBERGFELL

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Köln, Germany

Email: manuel.obergfell@grs.de

F. BERCHTOLD

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Garching, Germany

**Abstract**

Nuclear power plants (NPPs) with advanced reactor technologies, particularly small modular reactors (SMRs), are planned to be built in various countries worldwide. Due to the much lower power output of these reactor types in comparison to operating NPP units, the plants with SMRs are intended to be realized by multiple modules of the same type at a given site. Based on the type of the multi-module concept, the different SMR modules may share several systems, structures, and components (SSC), e.g., a joint building, or the electrical power supply, and/or a common team of operators. As an example, the NuScale VOYGR™-type SMR is being developed to share SSC for up to twelve modules.

For analysing the risk of multiple modules at a common nuclear site, GRS has developed a multi-module Level 1 PSA for a VOYGR™ SMR plant applying the commercially available PSA code RiskSpectrum®. The model enables the analysts to compare the risk from a single module to that of multiple, up to twelve identical modules located in the same building, sharing several SSC and the operator´s team. The manufacturer´s PSA of NuScale has been modified by an own analysis of initiating events (i.e., common cause initiators (CCIs) affecting multiple modules) and applying reliability data for systems and components from the German operating experience regarding single and/or common cause failures (CCFs). As a result, the core damage frequencies (CDFs) for a hypothetic nuclear site with only a single SMR module site and with twelve modules have been determined and compared. Multi-module cut sets with an important contribution to the overall risk have been identified, such as internal fire with inadvertent activation of the emergency core cooling system (ECCS) in all modules, CCF of all reactor recirculation valves (RRV) inadvertent activation block (IAB) valves in four modules, CCF of all the passive RRV opening function in all modules and an operator failure to initiate a necessary system in 1 out of 4 affected modules. Inter-module CCFs and human failures have been observed to be important risk contributors. Very important are, e.g., the CCF of main steam isolation and backup valves in four affected modules, human failure serving one out of two affected modules and the CCF of RRV IAB valves in four affected modules. The analysis of significant contributors to the overall multi-module risk appears to be beneficial for quantifying the main cut sets and the safety balance of the reactor concept.

## INTRODUCTION

Germany’s technical experience on NPPs meanwhile covers more than 40 years. In the past PSA analyses resulted in significant improvements in reactor safety and high level safety standards for German NPPs. The operating experience allows to deduce parameter values on the reliability of SSC for the corresponding reactor design. In this research and development activity the focus is on newly developed small modular reactor (SMR) designs. The PSA for SMR is different to the German NPP PSA as the PSA is not applied to reactor units in operation but to reactors in the design and/or licensing and construction phase. Therefore, the parameter values for the reliability of SSC are so far unknown. A common resolution of this issue is the use of parameter values for the reliability of comparable SSC in traditional NPPs. It is expected that these parameter values reproduce the correct order of magnitude for the reliability and, what is even more important, the correct proportion between the different components, e.g., a pump may fail 10 or 100 times more often compared to a valve. Unfortunately, the method does not allow to credit design modifications intended to improve the components. However, the PSA can help to improve system designs, e.g., it credits the design of multiple and diverse accident core cooling options.

Multiple modules or units of SMRs are expected to be installed at an individual nuclear site to reduce the costs of construction [1], maintenance, and operation. The NuScale SMR was intended to be built at least with four modules and with the possibility to implement up to twelve modules within the same building [2]. The modules are identical in design, and the operating team is assumed to be in charge for all modules in parallel. These two aspects are of major importance for the design of the multi-module PSA as CCIs, CCFs and human errors of the operating personnel will be more likely and/or may have a higher impact on the site CDF (SCDF) representing the risk metric of the GRS multi-module PSA. A comparison of the SCDF with the CDF of any (hypothetic) plant using one SMR unit/module can help quantifying the quality or balance of the installation or site safety concept to arrange multiple SMR modules. Furthermore, the multi-module PSA can be analysed to demonstrate the impact of CCIs, CCFs and operator errors to the SCDF. This may help to improve the site safety concept.

## PSA MODEL DESCRIPTION

The GRS PSA plant model is generally based on the information provided by NuScale regarding the design of the VOYGR™ SMR plant during the licensing process in the USA [2]. It is implemented in the RiskSpectrum® PSA plant model, Version 1.4.0. In this model, parameter values for the reliability of SSC [3], CCFs [4] and the frequency of initiating events mainly rely on the operating experience from traditional pressurized water reactors (PWRs) in Germany. The model considers common practice regarding operation and maintenance and includes the maintenance intervals in the installation for different SSC [5].

### Single-module PSA

The PSA for a hypothetic nuclear site with only a single reactor module has been implemented in RiskSpectrum® and is in line with recent international guidance provided in [6] and [7]. The model mainly consists of event trees (one event tree per initiating event) with function events, underlying fault trees, parameter values for the reliability of SSC and the frequencies of the initiating events.

#### Initiating events

Twenty initiating events from plant internal events and internal hazards have been identified including nine transients, one reactivity insertion scenario and six different loss of coolant accidents (LOCAs). In addition, internal fire, internal flooding and two events solely possible in shutdown mode are considered. Initiating events from external hazards and from hazard combinations have not yet been included in the model. Fifteen of the twenty initiating events had already been analysed by NuScale [2]. The additional initiating events have been identified by literature research of guidelines from the Netherlands [8], Germany [4], [9], [10] and IAEA documents about best practice. These events are:

1. Inadvertent control rod withdrawal (although this event is mentioned in [2], further investigations have not been found);
2. Coolant level and/or pressure increase in the steam generator (this initiating event has been analysed in [2] in conjunction with a general reactor trip);
3. Coolant level increase and/or pressure increase in the primary coolant system because of malfunction of the chemical and volume control system (CVCS) (this initiating event has been analysed in [2] in conjunction with a general reactor trip or a LOCA of the insertion line in the containment);
4. Small leak between reactor pool and containment (the frequency of this event is very low; it has been reasonably excluded in [2]);
5. Functional failure of the primary system circulation (the frequency of this event is very low; it has been reasonably excluded in [2]).

Although the contribution of these explicitly implemented initiating events to the CDF may be small, their implementation and quantification allow to prove the assumptions without any drawbacks.

#### Event trees

Most of the implemented event trees depend on the NuScale PSA [2]. The event trees for the additional initiating events could be generated based on the information about the SSC and the procedures known from German PWRs. The consequences are either core damage or no core damage.

#### Fault trees

The failure probabilities of the function events are calculated in the underlying fault trees. The fault trees had to be modelled without any knowledge about the NuScale PSA model implementation. However, the necessary information regarding the technical details of the SSC is available in the application documents [2]. Although the systems are in general less complex compared to traditional PWRs, the PSA models for German PWRs have also been used as reference. In very few cases a qualified assessment of the interrelation of components or equipment has been necessary. The systems modelled are:

1. Reactor trip system (RTS);
2. Decay heat removal system (DHRS);
3. ECCS;
4. CVCS and coolant supply systems;
5. Containment flooding and drainage system (CFDS);
6. Power supply systems including direct current, alternating current at different voltage levels and backup power supply.

The components of these systems have been compared to the components in German PWRs to quantify the component failure rates and CCF probabilities. The (rather low) human error failure probability has been taken from [2]. However, the human failure probability significantly increases in the GRS PSA model for multiple demands to manually initialize different systems. The human failure model was not found to have a significant impact on the result because most of the systems are started automatically, this holds for (a), (b), (c) and (f) in the list of modelled systems shown above.

### Multi-module PSA

The multi-module PSA is based on the IAEA guidelines for multi-unit PSA [2]. In a first step, the risk metric has been defined to be the CDF from one or more modules. This is a rather simple metric without any further information on the severity of the accident, e.g., containment bypass scenario. However, the event trees are much smaller and better readable by using this metric. In a second step, the initiating events are analysed for multi-module impact.

#### Multi-module initiating events and common cause initiators

All initiating events of the single-module PSA have been analysed for possibilities of CCIs which could impact multiple modules of the installation. A threshold cut-off criterion was applied to neglect the initiators with low core damage probabilities. Therefore, the single-module PSA was simplified without considering any success of human action or any success of systems shared by multiple modules. If the CDF of the initiating event has exceeded 0.1 % (2.4 E-09/ry) of the overall CDF, the initiating event has been chosen for multi-module analyses.

The following multi-module initiating events have been identified:

1. General transient: the very high frequency of general transients requires the consideration of non-correlated initiating events in two or three modules at almost the same time. Moreover, general transients in multiple modules are possible during internal fire or flooding events.
2. Loss of offsite power (LOOP);
3. Loss of supporting systems;
4. LOCA inside containment (because of a failure in the electronics of the heater for the pressurizer);
5. Containment leakage from/to the reactor pool (because of an event in the reactor pool); this scenario triggers a general transient without ECCS being available, e.g. with DHRS and CVCS failure, core damage is expected;
6. Inadvertent activation of the ECCS in all modules (because of a plant internal fire).

#### Multi-module event trees

A method is proposed where only 4 out of the 12 modules at the site are explicitly distinguished by considering their possible system failures. However, all twelve modules are included implicitly because the four modules can represent any of the twelve modules if the module is affected by one or more system failures of a required system to prevent a core damage. First, at the beginning of the transient, it is possible that more than four modules are affected by the initiating event; but during the transient it is sufficient to consider additional failures in up to four modules only because the contribution to the CDF is sufficiently decreasing for cut sets with multiple failures in multiple modules. Thus, the four modelled modules do not directly represent a module which is specifically located at a known bay in the reactor pool. In contrary to this usual direct assignment of each module in the PSA model to a module at a specific location in the system, the GRS model considers only the affected reactor modules. For example, the initiating event may affect all modules, but the first measure represented by the first function event may fail only in three of the modules, which could be the modules no. 3, 7 and 11 or 5, 6 and 8 or any other combination.

In the GRS model, however, all modules are treated equally and indistinguishably. All possible combinations of three out of twelve modules at the site are represented by the same cut set of the example. The correct quantification of the example cut set requires a multiplication factor of the binomial coefficient for all possible realizations at the site. The modules in this implementation are not distinguished by their location at the site but by the SSC failures in the module. This approach has several advantages, first, the event trees remain relatively small, and second, if the probability of the cut sets with many affected modules is below a reasonable threshold it is not necessary to generate fault trees for all twelve modules separately. In the GRS multi-module PSA, the fault trees have been quadruplicated to represent up to four affected modules. A decreasing contribution to the SCDF with an increasing number of affected modules has been observed by analysing the results. Therefore, the approximation of four affected modules is justified.

#### Multi-module fault trees

The multi-module fault trees are mostly copies of the single-module fault trees with a few modifications. The main modifications are:

1. Replacing the CCFs by CCFs of larger component groups;
2. Replacing the human failure model by a model considering increased failure probabilities if the operational team needs to act on several modules in parallel;
3. Function events based on systems with limited redundancy are implemented to fail if the number of affected modules is higher than the system redundancy;
4. Implementation of the binomial coefficient-based multiplication factors for the cut sets.

### Common cause failures

The CCF component groups of a single reactor module have been extended to component groups for twelve modules. The reasons for this extension are similar environment and manufacturing conditions and the identical design of the same components in different modules. Therefore, the groups can get rather large, e.g., the group of all EDSS batteries contains 96 batteries, the group of all ECCS trip valves contains 72 valves, the group of all CVCS makeup pumps contains 24 pumps. The component groups which had been determined for low group sizes in traditional NPPs before [4] have been enlarged to quantify the CCF probability of component groups over the whole plant. However, this comes along with an increased uncertainty, particularly in component groups based on very few documented CCF events or low operating periods, e.g., emergency equipment such as batteries.

### Human failures

A rather simple model for human error has been implemented into the multi-module PSA model. We expect the human failure to drastically increase if multiple modules need human actions at the same time. The implemented failure probabilities are presented in TABLE 1.

TABLE 1. HUMAN FAILURE

| Failure in module | Failure probability for request in one module | Failure probability for request in two modules | | Failure probability for request in three modules | Failure probability for request in four modules |
| --- | --- | --- | --- | --- | --- |
| Failure in one module | Same as in a single-module model | 0.10 | 0.50 | | 0.70 |
| Failure in two modules | - | 0.01 | 0.10 | | 0.24 |
| Failure in three modules | - | - | 0.01 | | 0.05 |
| Failure in modules | - | - | - | | 0.01 |
| Any failure | Same as in the single-module model | 0.11 | 0.61 | | 1.00 |

The model for human failures will be improved in a future version of the GRS multi-module PSA model.

## Model analyses and results

The model has been quantified applying the routines in RiskSpectrum®. The absolute cut-off threshold was set to 1.00 E-20 1/ry. The calculation took a few hours on a regular notebook. Internal initiating events during operation and during refuelling, internal fire and internal flooding events are analysed. The single-module CDF and multi-module SCDF, the multi-module correlation factor (MMCF) for comparison with the model of a single module, the main cut sets and the important risk contributors have been calculated. The MMCF, defined in Section 3.2, compares the SCDF contribution to the CDF within the multi-module PSA. The results are presented in the following sections.

### Contributions to the multi-module SCDF

Generally, the SCDF is an indicator for the overall CDF at the NPP site. However, at this first stage of the model development, the SCDF may differ orders of magnitude from the real value because of the limited level of detail and the use of conservative generic estimates and expert judgement. Major aspect of the present study of the SCDF is a comparison of the contributions to the SCDF by different initiating events as presented in FIG. 1.

*FIG. 1. Multi-module SCDF (in 1/ry) for different CCIs for full power plant in operational state.*

The current model does not represent a reactor concept with a balanced risk profile spread over different initiators. Moreover, the actual model shows high contributions from plant internal fire events. Regarding this result the authors recommend an update of the model improving the implementation of firefighting capabilities, e.g. crediting fire extinguishing systems and equipment, firefighters, etc. However, the model can be improved first to reduce conservative estimates and expert judgement focusing on important risk contributors mentioned in Section 3.4. One example of the use of expert judgement is the initiating event of containment leakage because of lacking information about the event. A water flow from the reactor pool into the containment due to a leakage will induce a reactor scram. The transient cannot rely on the ECCS because coolant might be lost over the leakage.

### Multi-module correlation factor

The multi-module model differs in a few aspects from the single-module model described in Section 2.2. Therefore, the SCDF deviates from the very simple approximation of 12 times the CDF of a hypothetic single reactor module presented in Section 2.1. In a comparison of the (single module) CDF and the multi-module SCDF the deviation can be quantified using the multi-module correlation factor (MMCF) defined here to be MMCF = SCDF/(12\*CDF), which can be calculated both for individual initiating events and for the total resulting CDF metrics.

The factor is the same as for all single-module specific initiating events, e.g., most of the LOCAs. Factors, which contribute to values below 1 for multi-module initiating events are the following:

1. Larger CCF groups mainly result in lower CCF values for a single module as the defect detection time is lower, and the probability that the defect exists in multiple components of a single module only and in none of the other modules at the same time is rather low.
2. A few multi-module initiating events have the same frequency as the initiating event in the single-module PSA, e.g., the LOOP providing a factor of 1/12 to the MMCF. This is different for initiating events like a LOCA, where the frequency is individual for each module. In such cases the multi-module initiating event frequency is about 12 times the frequency of a single module.

Factors which contribute to MMCF higher than 1 are:

1. Human error, which is increased if multiple modules are affected at the same time;
2. CCF in multiple modules in combination with an increased human error probability or limited equipment;
3. Limited equipment: A few systems are shared by multiple modules, e.g., CFDS, diesel generators, combustion turbine generator.

The MMCF is separately analysed for each multi-module initiating events, the result is shown in FIG. 2.

*FIG. 2. MMCFs for all multi-module initiating events.*

The MMCF is found to be higher than 1 for several CCIs with the highest value of more than 100. The result demonstrates the need for conducting a multi-module PSA; values based on expert judgement may differ substantially. The result can be averaged by weighting with the total contribution to the SCDF. The weighted average MMCF is found to be 1.30.

### Main cut sets

Basically, there are the following different types of main cut sets:

1. Core damage because of a module drop during the refuelling process: 1.3 E-06/ry;
2. Functional failure of the primary system circulation without stabilization after shutdown: 6.0 E-07/ry;
3. Internal fire with reactor trip and ESFAS failure in 6 modules, multiple operator failures in all affected modules:1.8 E-07/ry;
4. Internal fire with inadvertent coolant addition to the reactor coolant system (RCS), CCF of containment isolation valves (CIVs) of a single module and CCF of RRV or RVV IAB valves of a single module not switching its states: 1.7 E-07/ry;
5. Internal fire with inadvertent coolant addition to the RCS, CCF of RRV Inadvertent Actuation Block (IAB) valves of a single module and DHRS failure because of either CCF of all DHRS activation valves or all valves to isolate the main steam line in both steam generators of a single module: 3.8 E-08/ry;
6. Loss of all EDSS buses and CCF of all RRV IAB valves of a single module: 2.9 E-08/ry;
7. Inadvertent activation of the ECCS in all modules due to fire, CCF of all RRV IAB valves in four modules, CCF of all the passive RRV opening function in all modules and an operator failure to initiate a necessary system in 1out of 4 affected modules: 1.6 E-08/ry.

The cut sets (c) and (g) are fully multi-module cut sets based on a multi-module event trees.

### Important risk contributors

The main cut sets depend on system failures. These system failures are modelled in fault trees using basic events. Some basic events are very often found in main cut sets or are relevant for main cut sets with high core damage frequency. In the following, the basic events with the highest contribution to the core damage frequency are presented in the order of the Fussell-Vesely importance starting with the most relevant basic event for the PSA result (the probabilities of the basic events are presented for orientation):

1. Stabilization of the natural convection after shutdown: 5.0 E-01;
2. RSV is demanded to open in a single module: 5.0 E-01;
3. CCFs of main steam isolation and backup valves in 4 modules: 1.4 E-06;
4. CCFs of passive RRV opening in all modules: 1.0 E-02;
5. Combustion turbine generator fails during mission time: 1.6 E-01;
6. CCFs of RRV IAB valves (in 1 module):1.9 E-03;
7. Human failure to initialize a required system in 4 out of 4 affected modules: 1.0 E-02;
8. CCF of both diesel generator during mission time: 1.1 E-02;
9. Human failure to initialize a required system in 1 out of 2 affected modules: 1.0 E-01;
10. CCFs of CIVs for the isolation of a CVCS insertion line (in 1 module): 5.1 E-05;
11. Human failure to initialize a required system in 1 out of 3 affected modules: 5.0 E-01;
12. CCFs of main steam isolation and backup valves in 3 modules: 2.4 E-06;
13. CCFs of RVV IAB valves (in 1 module): 9.9 E-04;
14. CCFs of passive RVV opening in all modules: 1.0 E-02.

Although, the CCFs of main steam isolation and backup valves in 3 modules, (l), have a higher failure probability compared to the same event in 4 modules, (c), the impact of (c) is higher, because afterwards the crew need to activate required systems in 4 modules rather than 3 which is a higher challenge. CCFs in multiple reactor modules, (c), (d), (l), and (n) are found to be very important contributors to the multi-module risk. Moreover, human failure is a very important contributor if human actions are needed in multiple modules, (g), (i) and (k), e.g., human actions to add coolant to the primary coolant system via CVCS.

## CONCLUSION

A Level 1 multi-module PSA model for analysing the risk at a common site has been developed for a VOYGR™ SMR plant. The model is based on the commercially available PSA code RiskSpectrum®. The multi-module risk, in particular the SCDF, of 12 identical reactor modules has been compared to the risk of a hypothetic single module plant. The different modules are located in the same building, sharing several SSC and the operator´s team. The manufacturer´s PSA of NuScale has been modified by an own analysis of initiating events (i.e., CCIs) and applying reliability data for systems and components from the German operating experience regarding single and/or common cause failures. Multi-module cut sets with an important contribution to the overall risk have been identified, these are, e.g., inadvertent activation of the ECCS in all modules because of fire, CCF of all RRV IAB valves in four modules, CCFs of the passive RRV opening function in all modules and an operator failure to initiate a required system in 1 out of 4 affected modules. Inter-module CCFs and human failures have been observed to be important risk contributors, in particular, CCFs of the main steam isolation and backup valves in four affected modules, human failure serving one out of two affected modules and the CCF of RRV IAB valves in four affected modules. The analysis of significant contributors to the inter-module risk appears to be beneficial for quantifying the main cut sets and the safety balance of the reactor concept.

ACKNOWLEDGEMENTS

This research and development activity has been funded by the German Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMUV). The authors acknowledge the support and contributions by Gerhard Mayer, Marina Röwekamp and Jan Stiller.

References

1. BOARIN, S., RICOTTI, M.E., An Evaluation of SMR Economic Attractiveness, Science and Technology of Nuclear Installations, 1-8, 2014.
2. NUSCALE, Application Documents for the NuScale US600 Design, Revision 5, U.S.NRC, Rockville, MD, 2020, [www.nrc.gov/reactors/new-reactors/smr/licensing-activities/nuscale/documents.html](http://www.nrc.gov/reactors/new-reactors/smr/licensing-activities/nuscale/documents.html).
3. VGB POWERTECH E.V., Zuverlässigkeitskenngrößen für Kernkraftwerkskomponenten, Zentrale Zuverlässigkeits- und Ereignisdatenbank, TW 805-13, Essen, 2012.
4. FACHARBEITSKREIS (FAK) PROBABILISTISCHE SICHERHEITSANALYSEN FÜR KERNKRAFTWERKE, Methoden und Daten zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: Mai 2015, BfS-SCHR-61/16, Bundesamt für Strahlenschutz (BfS), Salzgitter, September 2016 (in German), <https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-2016091314090/3/BfS-SCHR-61-16.pdf>.
5. INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Multi-unit Probabilistic Safety Assessment, IAEA Safety Reports Series No. 110, Vienna, 2023.
6. ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT (OECD) NUCLEAR ENERGY AGENCY (NEA), Committee on the Safety of Nuclear Installations (CSNI), A Summary of Proceedings at the June 2022 Symposium on PSA for Reactors of Singular Designs, NEA/CSNI/R(2023)xy, Paris, in preparation 2024.
7. INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Specific Safety Guide, IAEA Safety Standards Series No. SSG-3, Rev. 1, STI/PUB/2056, ISBN 978-92-0-130723-1, Vienna, 2024, https://doi.org/10.61092/iaea.3ezv-lp4.
8. AUTHORITY FOR NUCLEAR SAFETY AND RADIATION PROTECTION (ANVS), Safety Guidelines, Guidelines on the Safe Design and Operation of Nuclear Reactors, Den Haag, 2015.
9. FACHARBEITSKREIS (FAK) PROBABILISTISCHE SICHERHEITSANALYSEN FÜR KERNKRAFTWERKE, Methoden zur probabilistischen Sicherheitsanalyse für Kernkraftwerke, Stand: August 2005, BfS-SCHR-37/05, ISBN 3-86509-414-7, Bundesamt für Strahlenschutz (BfS), Salzgitter, October 2005 (in German), https://[doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-201011243824/1/BfS\_2005\_SCHR-37\_05.pdf](https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-201011243824/1/BfS_2005_SCHR-37_05.pdf).
10. FACHARBEITSKREIS (FAK) PROBABILISTISCHE SICHERHEITSANALYSEN FÜR KERNKRAFTWERKE, Daten zur Quantifizierung von Ereignisablaufdiagrammen und Fehlerbäumen, Stand: August 2005, BfS-SCHR-38/05, ISBN 3-86509-415-5, Bundesamt für Strahlenschutz (BfS), Salzgitter, October 2005 (in German), https://[doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-201011243838/1/BfS\_2005\_SCHR-38\_05.pdf](https://doris.bfs.de/jspui/bitstream/urn:nbn:de:0221-201011243838/1/BfS_2005_SCHR-38_05.pdf).