Development of accident scenarios for shutdown probabilistic safety assessment

Marko Čepin [1], Anton Čauševski [2]

[1] Faculty of Electrical Engineering, University of Ljubljana, Trzaska cesta 25, Ljubljana,1000, Slovenia
marko.cepin@fe.uni-lj.si
[2] Faculty of Electrical Engineering and Information Technologies, Ss Cyril and Methodius University, Rugjer Boshkovik bb, Skopje, Macedonia
caus@feit.ukim.edu.mk

Probabilistic safety assessment is a standardized method for assessment of nuclear power plants safety and it is used intensively in the other technical fields where either safety or reliability is an important issue. The objective of this paper is to present one of the most important steps within the method of shutdown probabilistic safety assessment, which is a development of accident scenarios. In addition the objective is to show the application of the overall method and the results on a real example of existing models that were performed for a real power plant. The shutdown probabilistic safety assessment is presented with focus to its step of developing the accident scenarios. The models, which were developed for a particular power plant, are presented. The relations and the differences compared to full power probabilistic safety assessment models are discussed. The results show that the core damage frequency for different plant operating states varies significantly. In average, it is notably lower than the core damage frequency for the plant in full power operation. One can argue that the core damage frequency as a risk measure at full power plant operation is not comparable to the core damage frequency as a risk measure at other plant operating states, specially, to those with no fuel in the reactor, but the states with no fuel in the reactor are assessed separately within the analysis of the spent fuel pit, where its boiling frequency may be conservatively more appropriate risk measure than fuel frequency damage, knowing that either of them is not directly comparable to core damage frequency of states with fuel in the reactor. Although, the results show lower average of core damage frequency through the refueling outage, some states can be found with higher core damage frequency. The use of risk importance factors stays a question for future work, but at least for short plant operating states the uncertainties related with risk importance measures may be too large for their wider use.

I. INTRODUCTION

Probabilistic safety assessment is a standardized method for assessment of nuclear power plants safety at its steady state full power operation and it is used intensively in the other technical fields where either safety or reliability is an important issue [1, 2]. Different opinions about its usefulness have been expressed from its very beginning. While the overall concept itself was accepted after some years of professional discussions, the mathematical simplifications have never reached unified opinions of professionals involved. Integration of the mathematical theories and practical limitations, when applying them keeping in mind the real plant processes and procedures, represents a difficult issue with positive and negative features. But finally, the overall acceptance of probabilistic safety assessment was reached with publication of standards for performing it.

After decades of successful use, several extensions of the original methods were developed. One of important extensions that attracted significant attention was probabilistic safety assessment performed for other modes than full power operation of nuclear power plant [3 - 9]. As it is a complex method and related to several still open questions, the draft standard is still in its draft version [10].

I.A. Objectives and limitations

The objective of this paper is to present one of the most important steps within the method of shutdown probabilistic safety assessment, which is a development of accident scenarios. In addition, the objective is to show the application of the overall method and the results on a real example of existing models that were performed for a real power plant.

The objective is to show examples related with the refueling shutdowns, but other shutdowns could be evaluated using the same method and procedures. The main difference between refueling shutdown and some other shutdown is in the amount of the decay heat at the latter stages of the refueling shutdown and in reduced number of plant operating states at shutdown, where no refueling takes place. Namely, refueling shutdowns may last for a month or similar time (the order of magnitude is month), while other shutdowns can be of much shorter durations. They may last for an order of magnitude of days.

The methods were developed and applied for the purpose of analyzing nuclear power plants with pressurized water reactors. The application of the methods to other types of plants and to the plants with several reactors on the same site requires slight modifications, while the general concept can be followed for them, too.

Plant operating state without the fuel in the reactor is out of the scope of this paper, because the activities with spent fuel pit should be analyzed separately using separate methods.

The consideration of internal events is the focus of this paper, while the models for other groups of initiating events, i. e. for internal fires, for internal floods, for earthquakes and for other external events can be done separately using the related methods.

II. PROBABILISTIC SAFETY ASSESSMENT AND SHUTDOWN PROBABILISTIC SAFETY ASSESSMENT

Probabilistic safety assessment has been originally focused to three main questions:

- what can go wrong,
- how probable it is and
- how large are the consequences.

The main related methods, which are used for development of the models, whose analyses leads to answers about these questions, include:

- the fault tree analysis for evaluation of systems and functions,
- the event tree analysis for definition of interactions between systems and functions
- human reliability analysis for evaluation of the behavior of plant operators,
- common cause analysis for assessment of dependency between components and systems, because for possibility of evaluation of the probabilistic models, the independence of component failures in basic events is assumed in the first place,
- other methods supporting the upper methods including data analysis, uncertainty analysis, interaction with thermal hydraulic analysis for determining the success criteria for specific systems, decision-making methods, which are connected with interpretation of the results.

Fig. 1 shows an overview of probabilistic safety assessment with the main methods and main equations.

The main parameters are the following:

f_n - accident frequency,

f_{ASdef} - frequency of accident sequence AS_{def},

F - number of specific plant damage states in specific event tree,

E - number of event trees,

D - number of plant damage states,

f_{AS} - accident sequence frequency,

f_{IEk} - frequency of initiating event k,

P_{TOP} - top event probability,

P_{Bj} - probability of occurrence of basic event B_j,

J - number of basic events in a minimal cut set,

P_{MCSi} - probability of minimal cut set i,

I - number of minimal cut sets (for FT evaluation),

λ_{Bj} - operating failure rate of the equipment modeled in the basic event B_j,

p_{Bj} … probability of failure per demand of equipment modeled in basic event B_j,

T_{mBj} - mission time of equipment modeled in basic event B_j.

Several other parameters can direct the probability of occurrence of specific basic event.

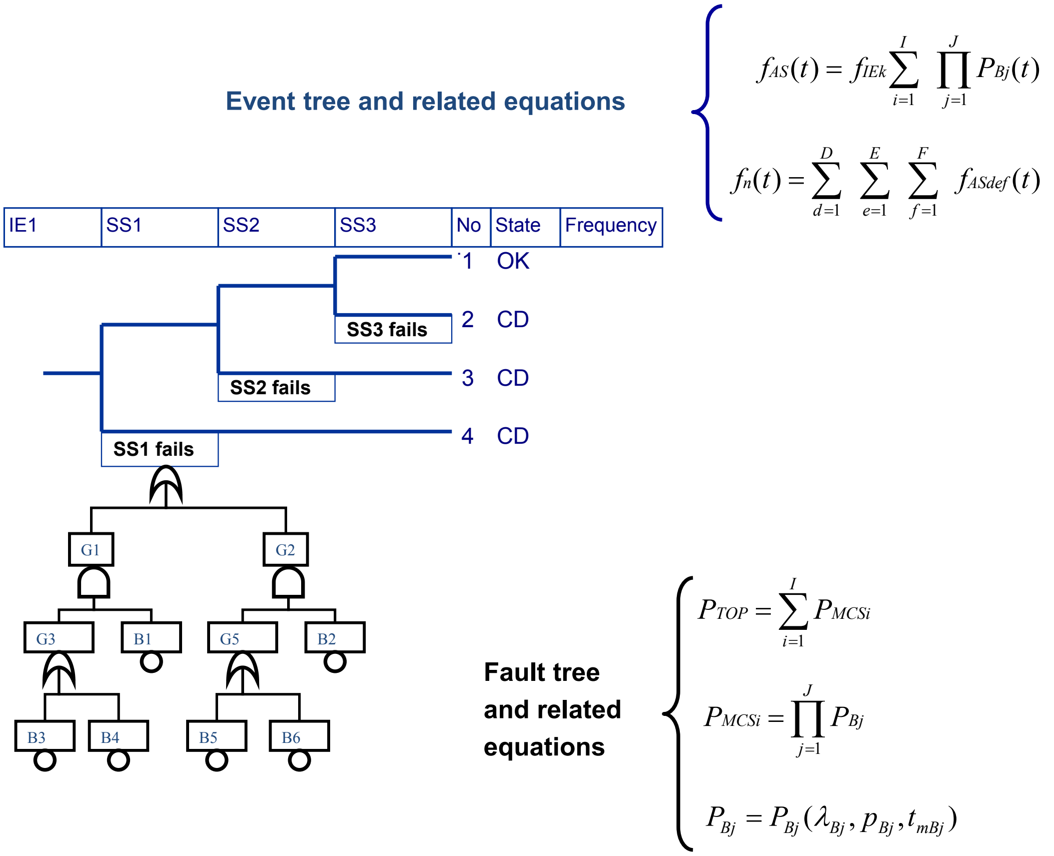
Event tree and related equations
$f_{AS}(t) = f_{IEk} \sum_{i=1}^{I} \prod_{j=1}^{J} P_{Bj}(t)$
$f_{n}(t) = \sum_{d=1}^{D} \sum_{e=1}^{E} \sum_{f=1}^{F} f_{ASdef}(t)$
IE1
SS1
SS2
SS3
No
State
Frequency
1 OK
2 CD
3 CD
4 CD
SS3 fails
SS2 fails
SS1 fails
G1
G2
G3
B1
G5
B2
B3
B4
B5
B6
Fault tree and related equations
$P_{TOP} = \sum_{i=1}^{I} P_{MCSi}$
$P_{MCSi} = \prod_{j=1}^{J} P_{Bj}$
$P_{Bj} = P_{Bj}(\lambda_{Bj}, p_{Bj}, t_{mBj})$

Fig. 1. Overview of probabilistic safety assessment.

II.A. Shutdown Probabilistic Safety Assessment

During the shutdown of the nuclear power plant, the plant systems operate primarily to maintain the core and the spent fuel cooling and to keep the fuel subcritical. The residual heat removal system is used for the decay heat removal during cold shutdown and refueling states. In general, the primary safety functions during the cold shutdown and refueling are the following:

- Decay heat removal with residual heat removal system.
- Reactor coolant system inventory control by keeping the reactor coolant system inventory at a level sufficient to sustain core cooling with residual heat removal.
- Reactivity control by keeping the shutdown subcritical conditions through boration of the reactor coolant system and having control rods fully inserted into reactor core.
- Reactor coolant system pressure and temperature control by keeping the reactor coolant system pressure and temperature within acceptable limits to enable continuous residual heat removal system operation and to prevent reactor coolant system boiling. This control is provided by reactor coolant system makeup and residual heat removal system.

The shutdown probabilistic safety assessment divides the overall shutdown period to separate and independently treated plant operating states. Even plant full power operation can be one of those states, the other can be reduced power operation and the hot standby and hot shutdown can be other plant operating states. Cold shutdown and refueling can be divided to any number of plant operating states keeping in mind that the plant parameters are assumed constant at specific plant operating state together with configuration of plant systems on one side and complexity of the models on the other side. In theory, the models would be more exact if 20 plant operating states or even more would be defined each with its own level of decay heat produced at its time interval and each with its specific configuration of systems that are operable and systems which are in standby and systems, which are out of operation for the maintenance. On the other side, the time consumed for development of such high number of models would exceed the benefits gained when getting the models, analyses and results out of these plant operating states.

Fig. 2 shows that the power related to the decay heat is conservatively assessed for the whole plant operating state based on the largest power related to the decay heat in this state.

Table 1 shows an example of plant operating states definition, where the related mode of operation is defined as the first number in the numbered code name and the serial number of plant operating state as the second number in the numbered code name. The second number is more important for modes, where more plant operating states is related with one mode. Actually mode 7 does not fully exist but the fuel out of the reactor is treated separately and this is out of the scope of this paper. For easier presentation of the results, the identification numbers for specific plant operating states may be consecutively numbered from power operation to shutdown states and back.

TABLE I. Plant operating states

Power Operation	Startup	Hot Standby	Hot Shut-down	Cold Shutdown			Refueling						No fuel in Reactor
POS-1-1	POS-2-1	POS-3-1	POS-4-1	POS-5-1	POS-5-2	POS-5-3	POS-6-1	POS-6-2	POS-6-3	POS-6-4	POS-6-5	POS-6-6	POS-7-1

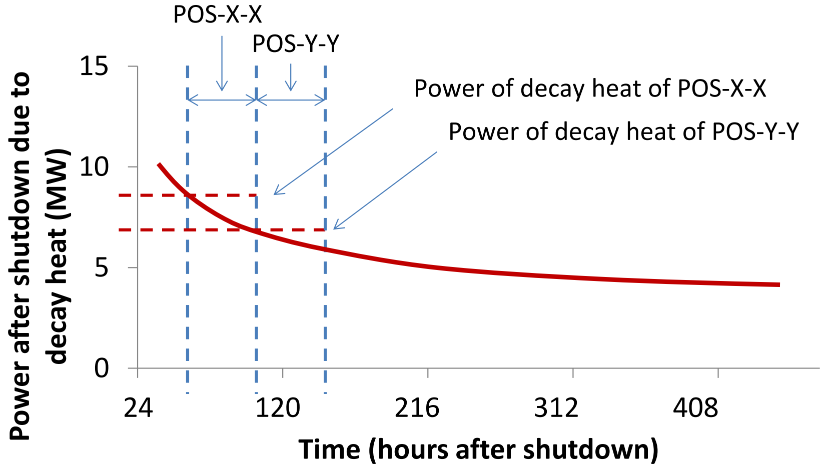

Fig. 2.Thermal power of the reactor related to the decay heat.

The method for performing shutdown probabilistic safety assessment is comprised of the following steps:

1. Definition and analysis of initiating events.

   Examples of initiating events include internal events such as loss of offsite power, loss of coolant accident, steam generator tube rupture, steam line break, loss of component cooling. For each plant operating state, the list of initiating events can be unique. For example, initiating events related to loss of coolant accident are not applicable in shutdown states, where the reactor coolant system is unavailable. Similarly, steam generator tube rupture is not applicable in these states, transients related to secondary side are not applicable in these states, as well as anticipated transient without scram. On the other hand, new initiating events related to loss of residual heat removal system, such as slow draining of reactor coolant system, rapid draining of reactor coolant system and loss of residual heat removal system may be important and should be considered. Vessel failure can be considered for operating states where reactor coolant system is still under pressure, but its frequency may be different due to different pressure.

   Identification of relevant situations is performed with review of existing studies and event reports. Their applicability to the specific plant operating state under consideration is needed to obtain a representative set of initiating events.

2. Accident sequence development and analysis (development of event trees).

Accident sequence is a sequence of events which starts from an initiating event and includes responses of safety systems or operator actions, which can be either successful or unsuccessful, and ends in a damage state or in an acceptable safe state. Successful or unsuccessful responses of safety systems and/or operator actions are represented as functional events. The most common damage state is core damage.
Initiating events frequencies are expressed in terms of number of occurrences per year. Here it is important to consider the time duration of specific plant operating state. For example, if plant operates 8766 hours in one year in a specific plant operating state, or if it would operate for half of this time in this state, the risk is not the same in both cases.
In order to be able to compare the core damage frequency among plant operating states durations, the initiating event frequencies need to be modified for each state considering the time duration of this particular state. The equation is applicable to determine the initiating event frequency in one state, if the frequency of another state is known and no other means are determined to assess the related initiating event frequency.

$$\mathrm{f}_{\mathrm{IEik}} = \mathrm{f}_{\mathrm{IEim}} \cdot \frac{T_{\mathrm{POSm}}}{\mathrm{T}_{\mathrm{POSk}}} \qquad (1)$$

where
$\mathrm{f}_{\mathrm{IEik}}$ - frequency of initiating event i in plant operating state k,
$\mathrm{f}_{\mathrm{IEim}}$ - frequency of initiating event i in plant operating state m,
$\mathrm{T}_{\mathrm{POSm}}$ - time interval of plant operating state m,
$\mathrm{T}_{\mathrm{POSk}}$ - time interval related to plant operating state k.

The upper equation bases on the fact that the mean core damage frequency over a certain time interval can be expressed as the average value.

$$CDF = \frac{\sum_{i=1}^{l} CDF_i \cdot T_i}{\sum_{i=1}^{l} T_i} \qquad (2)$$

where
CDF - overall core damage frequency,
CDF_i - core damage frequency of the i-th plant operating state,
T_i - the time duration of the i-th plant operating state,
l - the number of all plant operating states.

ASME draft standard [10] states the total number of hours in a year is 8766 hours. The overall time of all plant operating states (T) is the sum of durations of all plant operating states (T_1, T_2, $\ldots\mathrm{T}_l$). $\mathrm{T}=\mathrm{T}_1+\mathrm{T}_2+\ldots\mathrm{T}_l$. So the applicable equation for the calculation of initiating event frequencies from the known initiating event frequency of a certain plant operating state is the following.

$$\mathrm{f}_{\mathrm{IEik}} = \mathrm{f}_{\mathrm{IEi1y}} \cdot \frac{T_{\mathrm{POSj}}}{\mathrm{T}} \qquad (3)$$

where
$\mathrm{f}_{\mathrm{IEik}}$ – frequency of initiating event i in plant operating state k,
$\mathrm{f}_{\mathrm{IEi1y}}$ – frequency of initiating event i considering one calendar year,
$\mathrm{T}_{\mathrm{POSj}}$ – time interval of plant operating state j,
T – time interval of one year.

Functional events related to safety systems may change compared to their analogous events in power probabilistic safety assessment in terms of success criteria regarding the required number of operating equipment, in terms of operating equipment versus standby equipment and in terms of relying on loops or trains which may be out of operation in certain plant operating state. A larger number of functional events may be directly connected with human actions, so different procedures may require different functional events and even different structure of event trees.
The initiating event draindown during shutdown is similar to the initiating event loss of coolant accident during power operation and leads to conditions with degradation of cooling capabilities.

Examples of functional events that are specific in plant shutdown may include feed and bleed, gravity feed, long term cooling with water supplied to refueling water storage tank and alternative heat removal with portable equipment.

Event tree analysis is a method, which graphically represents accident sequences associated with a particular initiating event or set of initiating events [11, 12]. The event tree describes the logical connection between the potential successes and failures of defined safety systems and/or operator actions as they correspond to the initiating event and the sequence of events. The event tree is presented in details in many references and is not repeated here [1, 2].

3. Success criteria analysis.
   Success criterion is a term which defines the conditions for the safety system to operate successfully. The configuration of the plant changes and consequently the success criteria for the system changes when one train is out of operation due to the maintenance. Even in one plant operating states thee may be several plant configurations, the success criteria should be the most representative for the duration of the state.
4. System analysis (development of fault trees).
   System analysis as an assessment of the failure probability of the system or the system function is mostly performed by the fault tree method, which is presented in details in many references and is not repeated here [1, 2].
5. Human reliability analysis.
   Human reliability analysis includes assessment of human error probabilities for failure events that take place at specified conditions considering the plant state and written procedures, which is presented in details in many references and is not repeated here [13, 14, 15].
6. Parameter estimation analysis (data analysis).
   Parameter estimation analysis is a process, where the failure probabilities of equipment considered in PSA are determined using databases with generic data, databases with specific data and with consideration of selecting proper probabilistic model regarding the failure mode of respective components, the appropriate parameters and their uncertainty. It is presented in details in many references and is not repeated here [16].
7. Quantification and results interpretation.
   Quantification of the models gives the following main results:
   - overall core damage frequency (other accident frequencies may be evaluated such as spent fuel pit boiling frequency, or damage frequency of dry fuel casks, if applicable),

     $$CDF_{overal} = \frac{CDF_1 \cdot t_1}{t_{overal}} + \frac{CDF_2 \cdot t_2}{t_{overal}} + \cdots + \frac{CDF_{lastPOS} \cdot t_{lastPOS}}{t_{overal}} \quad (4)$$

     where:
     where: CDF_{overal} - core damage frequency over certain time interval (it can be refueling only, or it can be the time between consecutive plant shutdowns),
     t_{overal} - time interval considered,
     CDF_1 - core damage frequency for plant operating state 1 over time interval t_1,
     CDF_2 - core damage frequency for plant operating state 2 over time interval t_2.
     If the ratio t_l/t_{overal} is already considered within adjusted initiating event frequency, one should not forgot, that CDF_l*t_l/t_{overal} is not core damage frequency but it is core damage frequency weighted for the time duration of specific plant operating state.
   - frequencies of specific plant operating states,
   - frequencies for different sets of initiators such as internal events, for internal fires, for internal flood, for seismic events, for external flood and for other external events,
   - frequencies of specific initiating events in specific plant operating states,
   - frequencies of specific accident sequences,
   - minimal cut sets for all above listed points,
   - importance factors for basic events (e. g. component failure modes, human failure events), basic event groups (e. g. components, trains, systems, specific basic event groups such as human failure events, specific kinds of equipment such as valves, pumps, active components, passive components) for all above listed points separately.

It is expected that internal events are considered first, when performing the shutdown probabilistic safety assessment as an overall method, and then the models are done for internal fires, for internal floods, for earthquakes and for other external events, in addition.

III. MODELS, ANALYSES AND RESULTS

Two nuclear power plants examples were considered. Only the results of one plant are presented in this paper. Fig. 3 shows the core damage frequency weighted for plant operating state duration contribution for shutdown 1 with its specific plant operating states durations. The time durations of specific plant operating states are different for every other plant shutdown. Consequently, the respective curves (presented as an example on Fig. 3), which represent the core damage frequency weighted for plant operating state duration, are different for every other plant shutdown. Similarly, their averaged values are different for every other plant shutdown. In theory, such figures can be developed before the shutdown considering the planned plant operating states durations. After the plant shutdown, when the plant operating states durations are known, the analysis can be upgraded with replacement of planned with realized durations of specific plant operating states.

The results presented on Fig. 3 and the results, which are obtained for other shutdowns, show that the core damage frequency varies significantly among different plant operating states. In average, it is notably lower than the core damage frequency for the plant in full power operation. On the other side, there are couple of specific plant operating states, where the risk is significantly higher than the average and for some cases the risk of specific plant operating state may be comparable or even higher than the risk of the plant full power operation.

One can argue that the core damage frequency as a risk measure at full power plant operation is not comparable to the core damage frequency as a risk measure at other plant operating states, specially, to those with no fuel in the reactor, but the states with no fuel in the reactor are assessed separately within the analysis of the spent fuel pit, where its boiling frequency may be conservatively more appropriate risk measure than fuel frequency damage, knowing that either of them is not directly comparable to core damage frequency of states with fuel in the reactor.

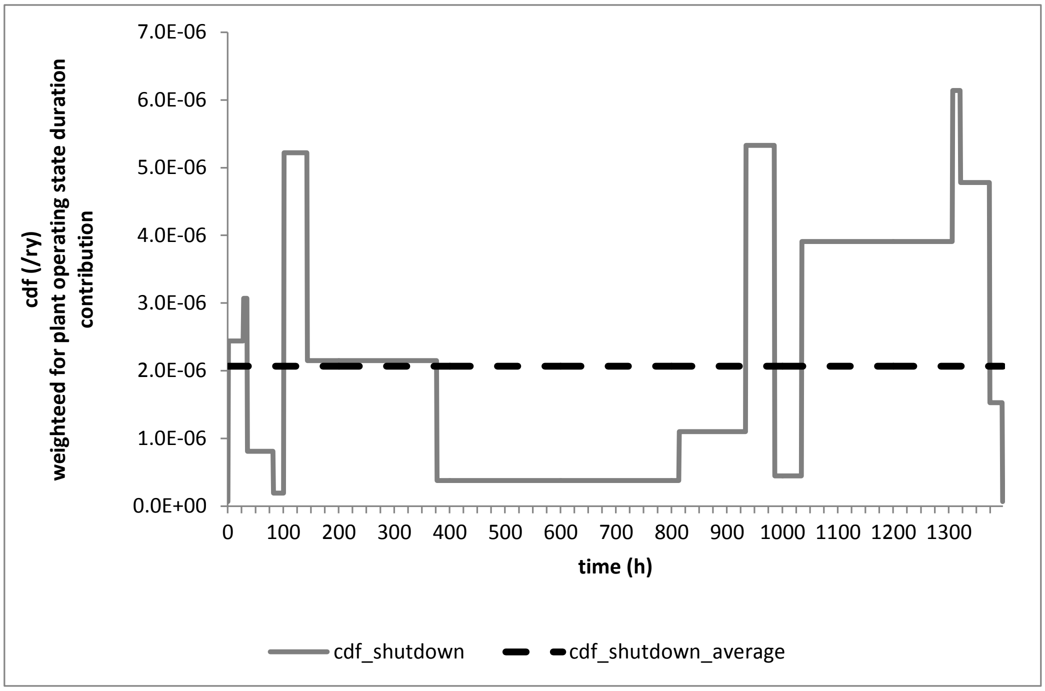

Fig. 3.Results: core damage frequency weighted for plant operating state duration contribution (shutdown 1).

IV. CONCLUSIONS

The objective was to present one of the most important steps within the method of shutdown probabilistic safety assessment, which is a development of accident scenarios. The method was presented. In addition, the objective was to show the application of the overall method and the results on a real example of existing models that were performed for a real power plant. The models, which were developed for a particular power plant, are presented.

Although, the results show lower average of core damage frequency through the refueling outage compared to core damage frequency at full power operation, some shutdown states can be found with higher core damage frequency compared to full power operation. Reduction of risk in these plant operating states is difficult because of less water above the reactor core, but human error probabilities that can be reduced by more training, can help. The use of risk importance factors compared through the plant operating states stays a question for future work, but at least for short plant operating states the uncertainties related with risk importance measures may be too large for their wider use.

REFERENCES

1. H. Kumamoto, E. J. Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists, IEEE Press, New York, 1996.
2. M. Čepin, Assessment of Power System Reliability, Springer, 2011.
3. NUREG-1449, Shutdown and Low-Power Operation at Commercial Nuclear Power Plants in the United States, US NRC, 1993.
4. NUREG/CR-6144, Evaluation of Potential Severe Accidents During Low Power and Shutdown Operations at Surry Unit 1, Vol. 1, US NRC, 1995.
5. K. Kiper, Insights from an All-Modes PSA at Seabrook Station, Proceedings of PSA2002, Detroit, 2002, pp. 429-434.
6. M. Čepin, R. Prosen, Probabilistic Safety Assessment for Hot Standby and Hot Shutdown, Proceedings of Nuclear Energy for New Europe 2008, NSS, 2008.
7. J. G. Kim, K. N. Lee, H. K. Lim, The methodology of the determination of the Plant Operating States of Lowe Power Shutdown Probabilistic Safety Assessment for the next-generation Nuclear Power Plants, Proceedings of PSAM12, Honolulu, Hawaii, USA, 2014.
8. M. Antončič, Ž. Bricman Rejc, M. Čepin, Probabilistic Safety Assessment of Shutdown and Refueling States, Proceedings of NENE2015, Nuclear Society of Slovenia, 2015.
9. A. Kim, J. Park, J. T. Kim, J. Kim, P. H. Seong, Study on the identification of main drivers affecting the performance of human operators during low power and shutdown operation, Annals of Nuclear Energy, 2016, Vol. 92, pp. 447–455.
10. Low Power and Shutdown PRA Methodology, 58.22 draft, 9/16/13, ASME, 2013.
11. I. A. Papazoglou, Mathematical Foundations of Event Trees, Reliability Engineering and System Safety, 1998, Vol. 61, pp. 169-183.
12. S. C. Swaminathan, C. Smidts, The Mathematical Formulation for the Event Sequence Diagram Framework, Reliability Engineering and System Safety, 1999, Vol. 65, pp. 103-118.
13. Handbook on HRA with Emphasis on NPP Applications, NUREG-CR/1278, NRC, 1983.
14. M. Čepin, DEPEND-HRA - A method for consideration of dependency in human reliability analysis, Reliability Engineering and System Safety, 2008, Vol. 93, no. 10, p. 1452-1460.
15. A. Prošek A., M. Čepin, Success criteria time windows of operator actions using RELAP5/MOD3.3 within human reliability analysis, Journal of Loss Prevention in the Process Industries, 2008, Vol. 21, no. 3, p. 260-267.
16. Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823, NRC, 2003.