On the Use of SPAR-CSN Model for Identifying Design Extension Conditions Type A Sequences. First Ideas.

César Queral[a], Sergio Courtin[a], Marcos Cabezas[a], Alberto García-Herranz[a], Julia Herrero-Otero[a], Enrique Meléndez[b], Miguel Sánchez[b], Rafael Mendizábal[b]
[a]Universidad Politécnica de Madrid (UPM), Madrid, Spain, *cesar.queral@upm.es*
[b]Consejo de Seguridad Nuclear (CSN), Madrid, Spain, *ema@csn.es*; *msp@csn.es*; *rmsanz@csn.es*

Abstract: After Fukushima accident, Nuclear Power Plants (NPPs) had to demonstrate their reliability increasing their safety requirements. One important requirement established in many countries is the analysis of the Design Extension Conditions (DEC) sequences to identify safety improving alternatives. This safety improvement of NPPs focuses on the conditions of multiple failures of the safety system excluded from Deterministic Safety Assessment (DSA). These DEC sequences are classified into DEC-A (Multiple failure followed by a safe shutdown) or DEC-B (Multiple failure followed by a fuel degradation).

As for the selection of DEC sequences, most, if not all, of the current practices/guidelines indicate that the selection of events to be analyzed shall be justified on the basis of deterministic and probabilistic arguments and of engineering judgment. Thus, there is a broad claim for the use of the Probabilistic Safety Assessment (PSA) models as a tool for the DEC identification process; nevertheless, no standardized methodology for PSA models has been found in the literature. For this reason, in the framework of the SPAR-CSN project to create a Standardized Plant Analysis Risk (SPAR) model for Spanish NPP, a novel methodology is proposed to identify DEC sequences making use of the PSA level 1 model for a generic plant.

The methodology proposed in this paper identifies the most important DEC-A Sequences from the PSA point of view. The outcome from the quantitative analysis shows a set of DEC-A sequences included on international DEC-based lists and, furthermore, some other sequences, not included in any other list of DEC-A sequences found, which would be interesting to analyze due to their quantitative risk significance.

---

1. INTRODUCTION

The Fukushima accident has brought, among others, an increment and improvement in the safety requirements for nuclear power plants (NPPs). One important requirement established in many countries is that the so-called Design Extension Conditions (DEC) need to be fully considered in the assessment of current and new advanced NPPs This safety improvement of NPPs focuses on the conditions of multiple failures of the safety system, included in the currently available safety guides widely in the world (e.g., as proposed by IAEA SSR 2/1). The associated applications and practices begin to emerge, given that the topic of DEC is being advanced rapidly both nationally and internationally. Nevertheless, these practices are still not comprehensive regarding the interface with the plant design basis, its role in the Defense-in-Depth, selection of requirements, impact on operating limits and conditions and/or selection of DEC sequences to be included in the analyses.

As for the selection of DEC sequences, most if not all, the current practices/guidelines indicate that "the selection of events to be analyzed shall be justified on the basis of deterministic and probabilistic arguments and of engineering judgment" and that "the selection process shall take into account all those events or combinations of events that cannot be considered extremely unlikely with a high degree of confidence and that might give rise to accident conditions more severe than those considered in design basis accidents" [1]. Thus, there is a broad claim for the use of the Probabilistic Safety Assessment (PSA) models as a tool for the DEC identification process.

The paper shows the first ideas and provisions with this aim (in section 4), as well as the results of the first application of this method to the SPAR-CSN generic model (in section 5). The next section describes the SPAR-CSN project and its objectives. Section 3 summarizes very briefly the current situation and guidelines used in other countries with the aim of identifying the list of Design Extension Conditions type A (DEC-A) sequences potentially to be considered in the Safety Analysis Report.

2. SPAR-CSN MODELS

The regulatory activity requires the oversight of licensee performance to be made from an independent position. This position is better served when the regulatory body develops its own methodologies and tools. In particular, in the matter of probabilistic risk analysis, even if the licensees' analyses are subject to peer-review and/or are reviewed by the regulatory body, it is very difficult to manage the large number of hypotheses and assumptions behind the model. Thus, the development of a PSA model for regulatory use improves the knowledge of the NPP risks and can be seen as an enhancement of the regulatory practice.

On this regard, the Spanish Regulatory Body (CSN), in collaboration with the Universidad Politécnica de Madrid (UPM), have been assembling its own generic Standardized Plant Analysis Risk (SPAR) model (SPAR-CSN) for 3-loop PWR-WEC designs. The current purpose of the project considers the elaboration of a standardized PSA model independent from the industry, providing a high-level view of risk in the evaluation of findings in Spanish NPPs, and intended to be comparable in scope to United States Nuclear Regulatory Commission (NRC) SPAR models [2,3,4]. To this end, the conclusions drawn from the comparison of the existing industry models are used to establish a common set of assumptions and standard modeling techniques to be used in CSN models [5]. The SPAR-CSN models aim to:

a) Better understand the main contributors to risk in Spanish NPPs.

b) Help in the prioritization of inspection and oversight tasks for Spanish NPPs through the analysis of systems' and components' importance.

c) Perform precursor analysis of operational incidents that occur in Spanish NPPs, in order to determine their closeness to a core damage scenario.

d) Provide an assessment of inspection findings within the Spanish regulatory system, SISC (Spanish acronym for Integrated NPP Oversight System).

The present paper introduces an extension of the scope of the initially foreseen applications to the goal of designing a suitable PSA-based methodology for DEC sequences.

3. CURRENT AND REGULAR PRACTICES IN DIFFERENT COUNTRIES

New practices and guidance begin to emerge, given that the topic of DEC is rapidly advancing in the regulatory arena. Despite this, there is a certain consensus regarding the definition of DEC-A, as sequences with multiple failures and conditions without significant fuel degradation, such as:

(1) Initiating events that could lead to a situation beyond the capability of safety systems that are designed for a single initiating event (e.g., multiple Steam Generator Tube Rupture (SGTR) in Pressurized Water Reactors (PWRs)).

(2) Multiple failures (e.g., common cause failures in redundant trains) that prevent the safety systems from performing their intended function to control the Postulated Initiating Events, PIE (e.g., Intermediate/Small Loss of Coolant Accident (LOCA) without actuation of High-Pressure Safety Injection (HPSI)).

(3) Multiple failures that cause the loss of a safety system while its system is used to fulfill the fundamental safety functions in normal operation (e.g., the same system for heat removal in accident conditions and during shutdown).

Nevertheless, these regulations do not normally identify lower frequency boundaries for DEC. Recurrent reasoning for this lack of quantitative criteria refers to the difficulties to obtain credible frequency values for low-frequency events, which may include multiple failures of equipment and human errors, as well as the large inherent ambiguities and uncertainties. In the end, most common practices for identifying events to be considered as DEC inevitably fall back on the judgment of experts, which adds further notable uncertainties [1,6,7].

Given that the set of DEC is specific to the reactor technology and to particular design options, identification and classification of events to be considered in design is the responsibility of the designer or the applicant for a license, and not to be imposed by the regulator who, however is required to verify the results.

Most, if not all, approaches for the identification of DEC without significant fuel degradation are declared to be based on the basic principle of "engineering judgment, deterministic assessments, and probabilistic assessments" [8]. Nevertheless, there are few, if any, specific details about how this basic principle is quantitatively applied, and only some qualitative rationales can be found. Examples of these are: "PSA would help identify dominant contributors to the overall core damage frequency and large release frequency, as well as an event that comes close to challenging the core and containment integrity" [9], "Regardless of the specific scenario, the designer should consider the known physical phenomena, which could challenge the fundamental safety functions" [9], and similar.

In conclusion, it seems that there is a need for an exhaustive and comprehensive method that, using a set of quantitative indicators (Figures of Merit, FoM), would be able to screen out the space of sequences, rank them and truncate the search by means of suitable cut-off rules (hopefully quantitative as well).

4. PSA BASED DEC-A IDENTIFICATION METHODOLOGY

In this section, the summary of a DEC-A identification process based on the PSA model is presented and discussed. This process is composed of the following steps (Sn) and criteria, see Figure 1:

S1 Select an Initiating Event (IE) from the list of IEs covered in the PSA model.

S2 Select all Sequences from Event Tree (ET) with at least 1 Failed Header (Sw1FH).

S3 Identify Sw1FH leading to Success (S) (e.g. application to Generic Transient (GT), Figure 2):

- These are candidates to be DEC-A sequences.
- Therefore, tag each identified sequence with "DEC-A" for the quantification process/code

S4 From each DEC-A tagged sequence identify all the sequences with further failures that lead to Core Damage (CD) (e.g. Figure 2):

- These are candidates to be DEC-B-related sequences of the tagged DEC-A sequence.
- Therefore, tag each identified sequence with "DEC-B".

S5 Quantify the frequency of every DEC-A tagged sequence, "DEC-A_freq". This step will make it possible to achieve a sorted list of sequences through the subsequent steps of the method.

Recurrent application of steps S1 to S5 would allow obtaining a comprehensive list of DEC-A sequences in conjunction with their related DEC-B.

S6 Applying a truncation criterion for DEC-A list reduction. The truncation criterion depends on the analysis target, a lower frequency limit requires the analysis of a greater DEC sequences set.

S7 Quantify the accumulated frequency of the DEC-B sequences related with each DEC-A sequence, "DEC-B_freq" (1). The method also postulates the use of the Conditional Core Damage Probability of the DEC sequence, "$CCDP_{DEC}$" (2), as Figure of Merit (FoM) for each element of the collapsed list.

$$\text{DEC-B\_freq} = \sum_{i=1}^{n} \text{Frequency}_i^{\text{DEC-B}} \tag{1}$$

$$CCDP_{DEC} = \frac{\text{DEC-B\_freq}}{\text{DEC-A\_freq} + \text{DEC-B\_freq}} \tag{2}$$

S8 Group similar DEC-A sequences and remove low-risk ones, DEC-B_freq < f0 or $CCDP_{DEC}$ < p1, and sequences covered by the Deterministic Safety Analysis (DSA). The outcome would be a collapsed list of DEC-A sequences and DEC-B-related sequences.

S9 Adding new sequences in terms of other eventual criteria not considered up to now (e.g., Large Early Release Frequency (LERF), Releases, Regulations, …)

S10 Application of steps S1 to S9 to other PSA models such as Fire, Spent Fuel Pool (SFP), External events, Low Power and Shutdown Probabilistic Risk Assessment (LPSD), …

S11 Adding new sequences in terms of other sources of DEC-A identification, such as Operating Experience, Expert Judgment, Regulatory Statements, Experience from other countries, dynamic PSA, etc.

Figure 1. Flowchart of the PSA-Based DEC-A Identification Process

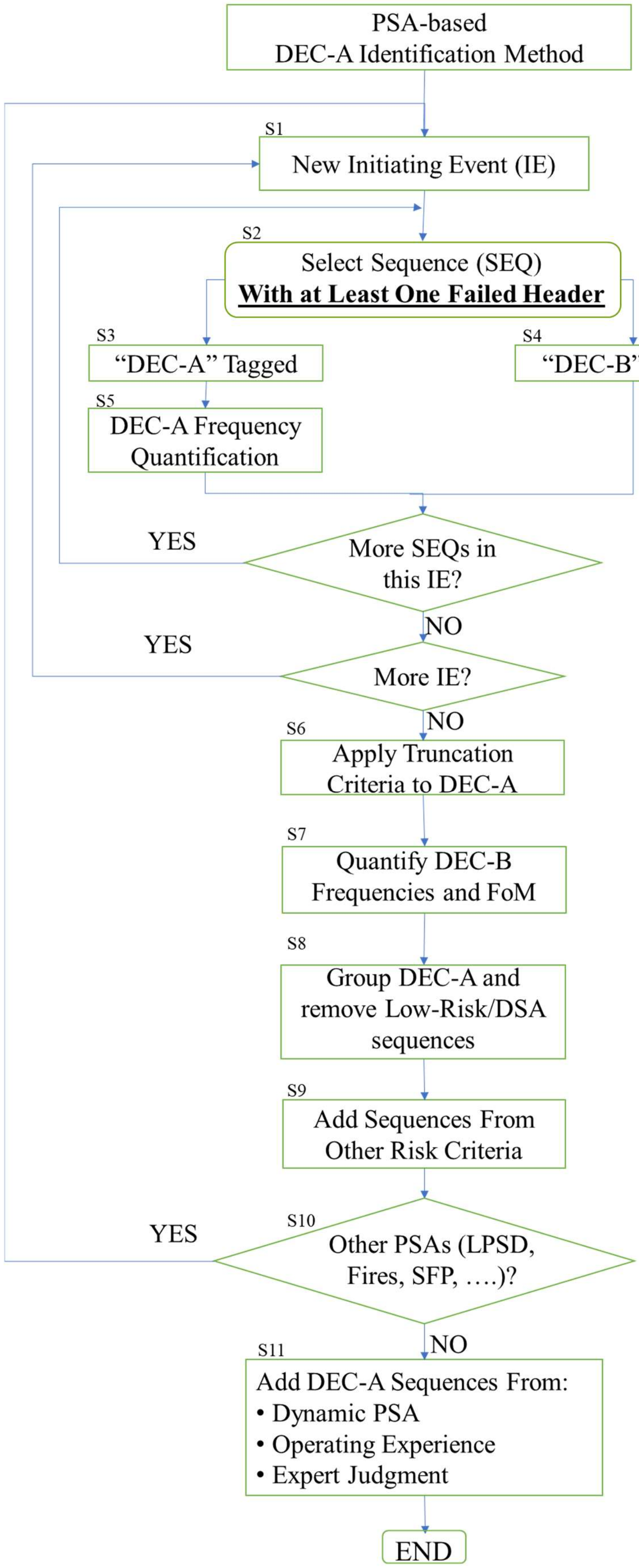
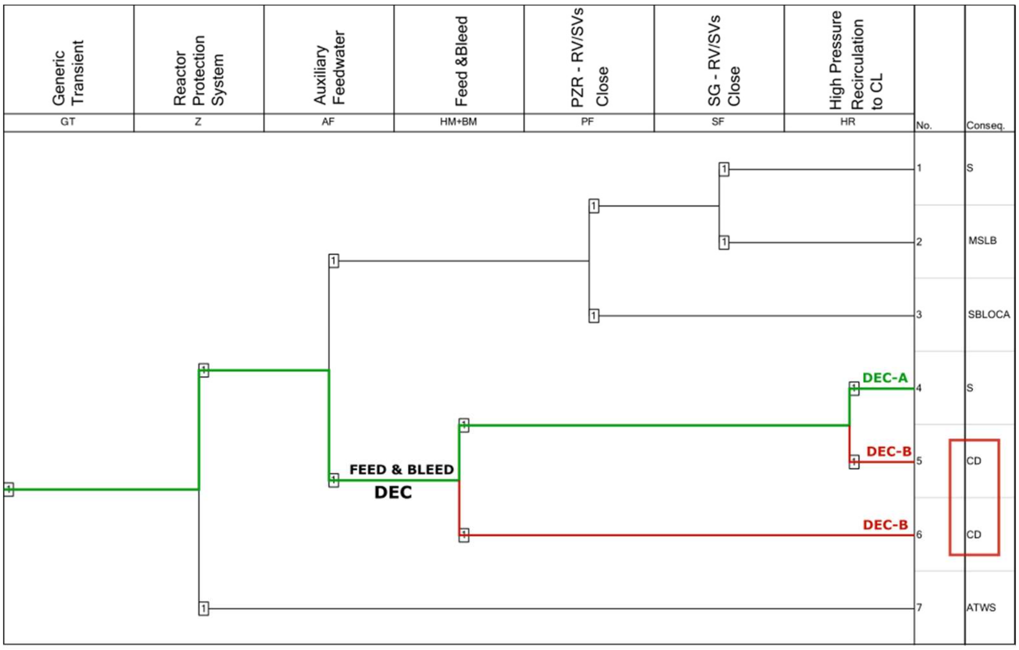


Figure 2. Application of Steps S1 to S4 of the Searching DEC Method to the GT ET.



5. APPLICATION. TENTATIVE LIST OF DEC-A SEQUENCES OBTAINED FROM SPAR-CSN MODELS

The application of the DEC-A identification methodology outlined in section 3 to the current SPAR-CSN generic model (level 1 PSA of internal events) presented in section 4, has allowed obtaining a qualified set of DEC-A sequences suitable to be compared with proposals of DEC-A lists currently managed in different contexts and regulations.

The initial full list of 185 DEC-A sequences identified as "success sequences with at least one failed header" on the SPAR-CSN model (the outcome of the recurrent application of steps S1 through S5 above), is reduced into an intermediate list of 69 sequences (step S6) considering a cut-off frequency of 1.0E-08 1/y. The purpose of the selected cut-off is to include all DEC-A sequences with a significant frequency and, in addition, to consider as many sequences recognized on international DEC-Based lists as reasonably possible.

At this point, DEC-B Frequency and FoM related with DEC-A sequences are quantified (step S7). The comparative FoM $CCDP_{DEC}$ is applied to the DEC-Based list in order to identify sequences with low/high relative risk.

Subsequent grouping of sequences according to similarity (steps S8 to S11), risk relevance, and other criteria (i.e., a quantitative informed expert judgment process) is implemented with the following steps:

(1) Taking out the sequences covered by DSA sequences (7 sequences) analyzed in the safety analysis report (e.g., success sequence of "Main Steam-Line Break (MSLB) ET" derived from the GT IE, Figure 2).

(2) Sequence grouping by similarity (e.g., GT with Total Loss of Feedwater (TLFW) and success Feed & Bleed (F&B) action, and LOOP with the success of the diesel generators to run, TLFW, and success F&B action) allows reducing the list from 62 to 14 sequences.

(3) The removal of 3 DEC-A sequences classified as low-risk sequences (DEC-B_freq < 1E-09 1/y or $CCDP_{DEC}$ < 1E-04) cause a reduction of the list to 11 sequences.

(4) Addition of 1 sequence by engineering judgement, Multiple SGTR.

This process leads to a final list of 12 DEC-A sequences. These sequences, included on table 1, are described below:

1. Station Blackout (SBO) with offsite power recovery.
2. Total Loss of Feedwater (TLFW) with successful Feed & Bleed action.
3. Steam Generator Tube Rupture (SGTR) consequential of a Steam-Line Break (SLB) with successful performance of the High-Pressure Safety injection (HPSI).
4. Small Break Loss of Coolant Accident (SBLOCA) consequential of a SLB with successful performance of HPSI during injection and recirculation modes.
5. Seal Loss of Coolant Accident (SLOCA) consequential of an SBO with offsite power recovery.
6. SBLOCA consequential of an SGTR with successful performance of HPSI during injection and recirculation modes.
7. Anticipated Transient Without SCRAM (ATWS).
8. SBLOCA/MBLOCA with failure to cool and depressurize Reactor Cooling System (RCS) with successful performance of HPSI on recirculation mode.
9. Loss of the Component Cooling Water System (LCCWS) with success of the Passive thermal Reactor Cooling Pump (RCP) seals or RCP seals injection by the Hydrostatic Test Pump.
10. SGTR with SG isolation failure and successful performance of Feed & Bleed (automatic injection).
11. SBLOCA/MBLOCA with HPSI failure and success to depressurize RCS and LPSI actuation.
12. Multiple SGTR.

The last column of the table 1 reflects whether the sequence has been included in any international regulation.

Table 1. List of DEC-A Identified by the Application of SPAR-CSN Based Methodology

No	Sequences	DEC-A_Freq. (1/y)	DEC-B_Freq. (1/y)	$CCDP_{DEC}$	Included on any DEC list?
1	SBO with offsite power recovery	7.6E-05	5.3E-08	7.E-04	Yes
2	TLFW + Success on F&B	5.8E-05	**7.8E-06**	**1.E-01**	Yes
3	SLB + SGTR + Success on HPSI	4.8E-05	1.1E-07	2.E-03	Yes
4	SLB + SBLOCA + Success on HPSI and HR	2.1E-05	**1.4E-06**	**6.E-02**	No
5	SBO + SLOCA with offsite power recovery	4.0E-06	3.7E-08	9E-03	Yes
6	SGTR + SBLOCA + Success on HPSI and HR	3.4E-06	**3.3E-06**	**5.E-01**	No
7	ATWS	1.9E-06	5.7E-08	**3.E-02**	Yes
8	SBLOCA/MBLOCA + Failure to depressurize RCS + Success on HR	8.8E-07	**1.2E-07**	**1.E-01**	No
9	LCCWS + Success on RCP seals	2.6E-07	7.2E-10	3.E-03	Yes
10	SGTR + Isolation Failure + Success on F&B (automatic injection)	1.8E-07	2.4E-08	**1.E-01**	Yes
11	SBLOCA/MBLOCA + HPSI failure + success to depressurize RCS and LPSI	3.3E-08	1.8E-08	**4.E-01**	Yes
12	MSGTR				Yes

The results show some DEC-A sequences with high relative risk, represented by the red marked values of DEC-B_Freq and $CCDP_{DEC}$ (see table 1). The most significant sequences from the point of view of risk are 2, 4, 6 and 8; these sequences are highly impacted by dependency between human actions which cause, most of the cases, a high $CCDP_{DEC}$ and DEC-B_Freq values.

Sequences 4, 6 and 8 from DEC-A list above are not included in any found international DEC-based list [1,10,11,12,13] and could be classified as high relative risk sequences ("$CCDP_{DEC-B}$" > 1E-02 and DEC-B_Freq > 1E-07 1/y). It is important to mention that the SBLOCA described in sequences 4 and 6 is caused by a failure to close a Pressure Operated Relief Valve (PORV) of the Pressurizer on SLB or SGTR situations.

The sequence "SBO with off-site power recovery" is the DEC-A sequence with highest frequency, but it is not one of the sequences with high relative risk. The main reason is the implementation of Passive Thermal Seals on the RCPs for SPAR-CSN model. This safety element also affects to the sequences "LCCWS + Success on RCP seals" and "SBO + SLOCA with offsite power recovery" decreasing the risk to cause core damage.

6. CONCLUSIONS

The main conclusions drawn up to now are summarized in the following points:

- The novel methodology developed in the framework of SPAR-CSN project allows standardizing the identification of DEC-A sequences on PSA level 1 models.

- The methodology allows to quantify the risk of DEC-A sequences by the FoM "$CCDP_{DEC}$" which, following the definition of DEC-A and DEC-B sequences, is the quotient between the cumulative DEC-B frequency and the cumulative frequency of all DEC-based sequences in which the DEC-B sequences are included.

- The results of this research show high similarity with other international DEC-Based lists, obtained by several regulatory bodies, and the selection by quantitative importance; 12 DEC-A sequences have been identified in the SPAR-CSN model, following the methodology, with high quantitative relevance.

- The results of the research reveal the existence of three potential DEC-A sequences, not included in any international DEC-Based list, with high relative risk ("$CCDP_{DEC-B}$" > 1E-02 and DEC-B_Freq > 1E-07 1/y). These sequences are:

  (1) SBLOCA consequential of a SLB with successful performance of HPSI during injection and recirculation modes,
  (2) SBLOCA consequential of an SGTR with successful performance of HPSI during injection and recirculation modes, and
  (3) SBLOCA/MBLOCA with failure to cool and depressurize RCS with successful performance of HPSI on recirculation mode.

  The results also allow for to grade of another four high relative risk DEC-A sequences ("$CCDP_{DEC-B}$" > 1E-02), included on international DEC-based lists. It is important to remark the influence the dependency between human actions on the potential risk of these sequences.

Acknowledgments

The UPM group acknowledges the technical and financial support granted by the CSN.

References

[1] Consejo de Seguridad Nuclear (CSN), "The analysis of design basis accidents at nuclear power plants", Instruction IS -37, (2015)

[2] H. Watanabe, S. Sancaktar, S. Dennis. "Generic PWR SPAR Model White Paper" (2018) https://www.nrc.gov/docs/ML1900/ML19008A133.pdf

[3] NRC. Risk assessment of operational event. Handbook. Volume 3 - SPAR model reviews, 2nd edition (2010).

[4] NRC, "SPAR Model Development Program", https://www.nrc.gov/docs/ML1029/ML102930134.pdf

[5] E. Meléndez, M. Sánchez-Perea, C. Queral, J. Mula, A. Hernández, C. París. "Standardized Probabilistic Safety Assessment Models: First Results and Conclusions of a Feasibility Study". 13th International Conference on Probabilistic Safety Assessment and Management (PSAM 13), Seoul, South Korea, 2-7 October 2016.

[6] General Nuclear System Ltd., CGN, "Design Extension Conditions and Severe Accident Analysis", UK HPR1000 DGA Project Preconstruction Safety Report, Chapter 13, (2020).

[7] C. Ma, Y. Ma, J. Du, "Study on PSA Application in VVER NPP Design Extension Condition Identification", 28th International Conference on Nuclear Engineering (ICONE-28), online, (2021).

[8] IAEA, "Deterministic Safety Analysis for Nuclear Power Plants", Specific Safety Guide SSG-2 (Rev. 1), (2019).

[9] H. Jiang, "Proceedings of the 20th Pacific Basin Nuclear Conference, Volume 1", Springer Singapore, 2017.

[10] P. Kral, "Analysis and Implementation of Design Extension Conditions (DEC) at Czech NPPS and Contribution of DEC to Enhancement of Defense-In-Depth", NURETH-18, Portland, United States, (2019).

[11] A. Prošek, M. Uršič, "Review of Design Extension Conditions Experiments and Analyses for Non-degraded Core", Journal of Energy, Volume 68 Number 2-3, 113-114, (2019)

[12] HPC, "Design Extension conditions A (DEC-A) - Multiple Failures Analysis", UK EPR Preconstruction Safety Report 3, Sub-chapter 14.5, (2017).

[13] STUK, "Olkiluoto 3 – FSAR Review Report", STUK, (2019)