The Problem of Safety Margin Assessment within the Risk-Informed Regulation

CSN

Colección
Otros Documentos
41.2017

CSN CONSEJO DE SEGURIDAD NUCLEAR

The Problem of Safety Margin Assessment within the Risk-Informed Regulation

J. M. Izquierdo Rocha
J. Hortal Reymundo
M. Sánchez Perea
E. Meléndez Asensio

Modeling and Simulation Area (MOSI), Deputy Direction of Nuclear Technology (STN), Nuclear Safety Direction (DSN), Nuclear Safety Council (CSN)

CSN CONSEJO DE SEGURIDAD NUCLEAR

Colección Otros Documentos
ODE-04.23

Edita y distribuye:
Consejo de Seguridad Nuclear
C/ Justo Dorado, 11. 28040 Madrid. España
www.csn.es
peticiones@csn.es
Maquetación: Composiciones RALI, S.A.
www.rali.es
Depósito legal: M-294-2017

Table of contents

1. Introduction and background. On the need of an Integrated Safety Margin Assessment within RIR 17

2. FirstPilot applications. CSNI Safety Margin Action Plan (SMAP) 23
2.1. Summary of SMAP 25
2.2. Probabilistic evaluation of safety margins 26
2.3. Main results of SMAP 29
2.4. CSN MOSI participation at the SMAP Group 30

3. First Pilot applications. The follow-up of SMAP: the SM2A exercise 31
3.1. Adaptation of the SMAP framework to SM2A 34
3.2. Development of the SM2A exercise 37
3.3. Lessons learned and conclusions from SM2A 39
3.4. MOSI/CSN participation and lessons learned as a result of the SM2A 41

4. Present Status of Integrated Methods and SM applications 43
4.1. MOSI/CSN Proposal: Integrated Safety Assessment methodology 45
4.2. Specific developments for characterization of safety margins 49

5. SM2A exercise. CSN analysis of the Loss of Component Cooling Water scenario 51
5.1. Description of the scenario 53
5.2. Sequence screening 54
5.3. Simulation codes 56
5.4. Probabilistic calculations 58
5.5. Modification of the sequence models 61
5.6. Modification of some header models 63
5.7. Base case simulations 66
5.8. Uncertainty analysis 68
5.9. Evaluation of exceedance frequency (results) 72

Appendix A. Comparison exercise on uncertainty analysis methods 75
A.1 System description 79
A.2 1st. analysis case: automatic protection 81
A.3 2nd. Analysis case: manual protection with dynamic dependent distributions 86
A.4 Overall conclusions of the exercise 92

Presentación

Presentación

Las tareas propias de un Organismo Regulador son específicas y distintas de otras tareas relacionadas con la seguridad propias de los titulares y las ingenierías al servicio de las instalaciones objeto de la regulación. Por ello, los organismos reguladores y sus Organizaciones de Apoyo Técnico (TSO en sus siglas en inglés) requieren de herramientas y métodos específicos.

El chequeo de la calidad, completitud y consistencia de los análisis que los titulares presentan como soporte de sus solicitudes es el principal objetivo de las evaluaciones del Regulador. En esta tarea, la disponibilidad de métodos y herramientas que permitan un enfoque integrado y cuantitativo (y por ende mas objetivo), permite optimizar los recursos del CSN en el ámbito de la evaluación de seguridad del diseño y la operación y conseguir una mayor garantía de que las instalaciones funcionan con un nivel de riesgo aceptable. Esto aplica de modo particular a asegurar que los aspectos deterministas y probabilistas estén adecuadamente acoplados puesto que ambos son inherentes al concepto de riesgo.

Sin embargo y como es bien conocido, es fácil hacer un mal uso de las probabilidades, lo que contribuye a menospreciarlas y a perder la mayor objetividad de lo cuantitativo. A pesar de ello, una reflexión elemental llega en seguida a la conclusión de que los problemas de optimización de protecciones hacen inevitables evaluaciones probabilistas, ya sean cuantitativas o cualitativas, estas últimas dependientes en exceso del subjetivo juicio de ingeniería. De ahí la necesidad de que el organismo regulador sea competente en discriminar los análisis cuantitativos buenos de los mediocres, dadas sus implicaciones en el diseño y la operación de las plantas.

Históricamente, el licenciamiento basado en los análisis de accidentes base de diseño siguiendo la llamada metodología determinista (DSA en sus siglas en inglés) se demostró pronto insuficiente para abordar otros aspectos de la seguridad, más relacionados con la operación que con el diseño de la planta. El accidente de Three Mile Island no hizo sino acentuar la necesidad de desarrollar los ya incipientes análisis de riesgo, comúnmente conocidos como Análisis Probabilistas de Seguridad (APS o, en inglés, PSA), no como reemplazo sino como complemento de los análisis deterministas. La dificultad de combinar de manera adecuada la aplicación de ambos tipos de análisis manteniendo la consistencia entre ellos se ejemplifica en dos problemas de especial relevancia en relación con la seguridad de las instalaciones:

1. Hasta qué punto y en qué etapa del análisis, los resultados del PSA son sensibles a cambios significativos en criterios de iniciación de sistemas de seguridad que tienen un impacto evidente en el DSA.

2. Hasta qué punto ambos tipos de análisis, DSA y PSA, recogen adecuadamente distintos comportamientos del equipo de operación de una instalación, particularmente en relación con los retardos en la realización de operaciones manuales.

Partiendo de este planteamiento y utilizando estos dos problemas como hilo conductor, el conjunto de publicaciones del que este documento forma parte, describe y actualiza con distinto grado de detalle, el proceso seguido en el actual área MOSI y sus grupos predecesores, para desarrollar los distintos elementos metodológicos y computacionales que han dado lugar a la metodología AIS (Análisis Integrado de Seguridad; ISA, Integrated Safety Assessment en inglés) y a la plataforma SCAIS (Sistema de Códigos para AIS) en su estado actual.

La metodología ISA se basa en un enfoque combinado de los aspectos deterministas y probabilistas del análisis de seguridad y pertenece a la categoría de las llamadas metodologías integradas de las que existen diversos planteamientos a nivel internacional.

Las herramientas de simulación han ido cubriendo sucesivamente aspectos de operación normal, accidentes con fenomenología bifásica, accidentes severos y actuaciones de los operadores. Simultáneamente se ha ido aumentando la capacidad de automatizar el uso de dichas herramientas para realizar simulaciones en árbol en las que la ocurrencia o no de determinados sucesos da lugar a distintas posibles evoluciones de una planta afectada por una situación anómala o accidental.

Los desarrollos teóricos que dan fundamento a la metodología se han ido implantando en paralelo con los recursos computacionales y la participación en diversos programas internacionales ha sido de capital importancia para mantener una línea de trabajo consonante con las tendencias más avanzadas en materia de análisis de seguridad.

Todo ello ha sido realizado en su mayor parte con la colaboración del Departamento de Energía y Combustibles de la Escuela Técnica Superior de Ingenieros de Minas de la UPM (Universidad Politécnica de Madrid), y con la empresa NFQ Solutions (anteriormente, Indizen Technologies).

Este documento forma parte de una colección de publicaciones del CSN, que resume todo este proceso de adquisición de métodos y herramientas específicos con los objetivos anteriores. Esta colección incluye dos volúmenes principales:

- *«CSN Experience in the Development and Application of a Computer Platform to Verify Consistency of Deterministic and Probabilistic Licensing Safety Cases.*
  Volume I. General Approach and Deterministic Developments»

- *«CSN Experience in the Development and Application of a Computer Platform to Verify Consistency of Deterministic and Probabilistic Licensing Safety Cases.*
  Volume II. Probabilsitic Developments and Applications»

dedicados respectivamente a los aspectos determinista y probabilista. Estos documentos describen el contexto, propósito, historia, modos de uso en distintas aplicaciones, ejemplos, etc. del método ISA en sus vertientes determinista y probabilista, pero no incluyen detalles técnicos de importancia, particularmente los de modelación matemática.

Por flexibilidad documental, los aspectos de detalle del volumen I se han editado con títulos independientes, pero pueden ser considerados como anexos. Están por tanto orientados a los usuarios del sistema informático que quieran conocer con precisión sus fundamentos y pueden ser considerados como la parte teórica de sus manuales de usuario. Contienen por tanto y de manera inevitable aspectos redundantes con el volumen I, pero descarga a éste de detalles que impiden una lectura más accesible.

El documento:

- *«The Importance of Accident Time Evolution in Regulatory Safety Assessment. Independent, Quantitative Tools and Methods at CSN to Ensure Adequate PSA/DSA Applications»*

desarrolla de modo preciso y en mayor profundidad los aspectos técnicos de la metodología y herramientas ISA en su versión actual, aportando teorías y herramientas de simulación, incluyendo numerosos desarrollos matemáticos y detalles adicionales de su simulación. Asimismo, describe sus aplicaciones para el chequeo cuantitativo de los análisis de licenciamiento en su vertiente determinista.

Y el documento:

- *«The Problem of Safety Margin Assessment within the Risk Informed Regulation»*

que sigue, presenta las principales conclusiones de la aplicación a la evaluación de Márgenes de Seguridad. Es ésta una aplicación muy relevante para al licenciamiento en la que las técnicas integradas son imprescindibles, y donde CSN-MOSI ha tenido una activa participación internacional.

El trabajo se realizó en el marco del grupo de trabajo SMAP (Safety Margin Action Plan) de NEA/CSNI al que se le encomendó la tarea de explorar conceptos y métodos que sirvieran de base para la cuantificación de posibles pérdidas de márgenes ante cambios significativos en las plantas. Posteriormente, se realizó un ejercicio piloto de aplicación de dicha metodología (proyecto SM2A, SMAP Framework

Assessment and Application) relativo a una propuesta hipotética de modificación de diseño de aumento de potencia.

Sobresale por ser la primera aplicación cuantitativa completa de la metodología ISA, entonces en primera versión, analizando sus detalles matemáticos, incluidos los desarrollos para el tratamiento de las incertidumbre temporales, una de las características diferenciadoras de las herramientas y métodos integrados.

Se analizan también todas las posibles implicaciones de los márgenes de seguridad, y se actualiza la situación al día de hoy.

Abstract

Abstract

The process of Safety Margin Assessment, as proposed in the Safety Margin Action Plan (SMAP) framework, is based on the identification of the Risk Space and the extensive application of uncertainty analysis methods to obtain an estimate of the exceedance frequency of specified safety limits, Safety Limit Exceedance Frequencies (SLEF). The Risk Space can be understood as an extension of both the Probabilistic Safety Assessment (PSA) event trees and the design scenarios intending to include every possible malfunction susceptible to challenge any safety limit of interest.

The Safety Margin Assessment Application (SM2A) expert group and its predecessor SMAP were created by the Committee on the Safety on Nuclear Installations (CSNI) of the NEA/OECD. The specific mandate of SM2A was to explore the practicability of the SMAP framework. To this purpose, the Task Group on SM2A carried out a pilot application project, completed late in 2010, to compute the increase in SLEF resulting from a 10% power uprate at Zion NPP (PWR-4 loop Westinghouse design). Each participant analyzed a particular event tree according to the PSA of the plant.

The participation of CSN in SM2A project included a sound collaboration of CSN with Universidad Politécnica de Madrid (UPM) and NFQ Solutions, to perform an analysis of sequences of Loss of Component Cooling Water System (LCCWS) applying the Integrated Safety Assessment methodology (ISA). This methodology aims at computing the contribution to SLEF from the sequences stemming from one or more initiating events. For this purpose ISA carries out an automatic delineation of Dynamic Event Trees (DET), and allows accounting of the uncertainties of the sequences. These uncertainties include time variability (as in, e.g., human actions or stochastic phenomena) and parameter values (break area, thermal power, pressures, mass flows, etc.). The method, developed by the Modeling and Simulation (MOSI) branch of the Spanish Nuclear Regulatory Body, entails several simulations of DET sequences in the application presented in this report.

I. Introduction and background. On the need of an Integrated Safety Margin Assessment within RIR

I. Introduction and background. On the need of an Integrated Safety Margin Assessment within RIR

In recent years, the international nuclear community is becoming more and more concerned about the possibility that significant changes in plant design or in operation strategies result in adverse side effects usually referred to as "erosion of safety margins". A number of initiatives have been launched to address this problem due to the increasing number of plants applying for power uprates, life extensions, increased fuel burn-up, etc., where some voices claim that, even complying with applicable regulations, there could be an unacceptable loss of safety margins. Moreover, the development of new designs for nuclear power plants where the existing technical regulations for LWRs are not necessarily applicable raises the need to establish criteria for determining what is an acceptable level of safety.

A second reason for the discussion about safety margins is the increasing trend to apply the so-called Risk-Informed Regulation (RIR). From the pioneering Regulatory Guide 1.174 of the USNRC, most safety standards and guides on this matter ask for "maintaining enough safety margins" as a condition for acceptability of any change being licensed in the framework of RIR.

For these and other reasons, the term "safety margin" has become a keyword when discussing about the overall safety of the plants but there is still much confusion about the use of this term, mainly because it is not always used with the same meaning.

The introduction of safety margins in traditional engineering is a protection design technique aimed at providing some additional protection capability beyond the one that is considered strictly necessary. The benefit of using safety margins is two-fold. On the one hand, they allow accommodating tolerances for little known phenomena, uncertainties in model data, variability in initial or boundary conditions, and so on. On the other, they result in a significant simplification of the design methods as they allow splitting the design in several decoupled stages where the applicable criteria are not too closely linked to the details of the phenomenology considered in the design analyses.

This approach, essentially deterministic, is considered conservative in most cases and, therefore, provides confidence that the protection is able to cope with or to mitigate challenging situations, including some that were not considered in the design analyses.

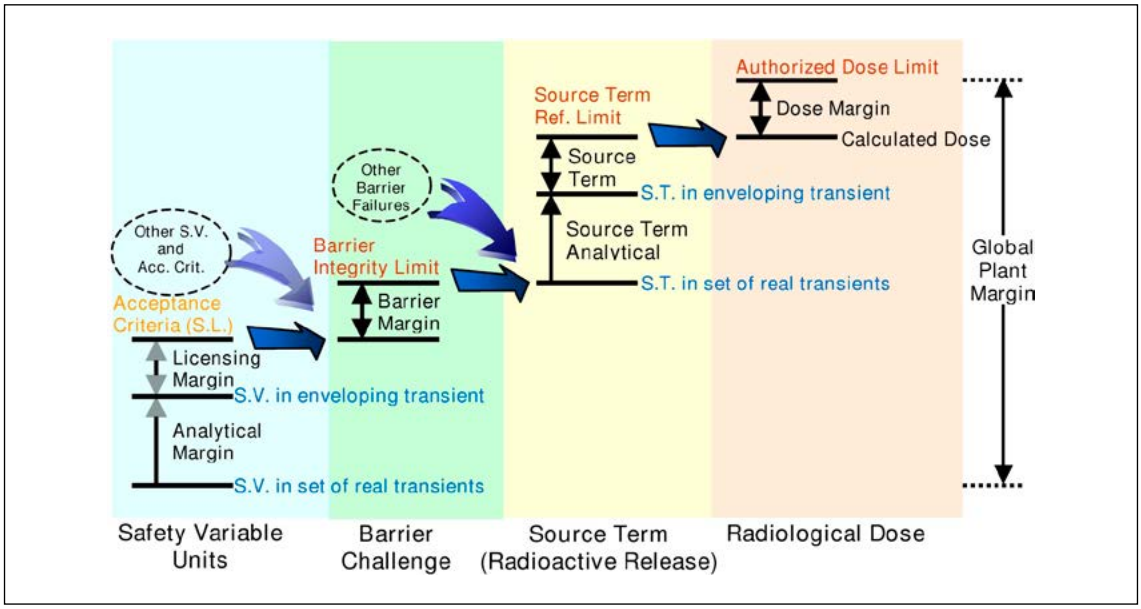
In addition, it is convenient for developing safety regulations. This idea was also applied from the beginning in the nuclear industry and, in particular, in the analysis of Design Basis Transients and Accidents (DBT&A, from now on referred to as DBT) where the capabilities of the protection are assessed. A set of well defined, enveloping scenarios, classified into a few frequency classes, are taken as design basis

for the protection and a set of safety variables are used as damage indicators or as indicators of challenges to the protection barriers. For this limited set of design basis scenarios it is possible to define class-specific acceptance criteria in terms of extreme allowed values of the safety variables, also called safety limits.

In this context, the concept of safety margin is applied on a scenario-specific basis and its meaning can be agreed without much difficulty. However, even at single scenario level, a great variety of margins appear and all of them can be properly called safety margins. Figure 1 tries to represent these margins and how they relate to each other.

The two stages of a typical DBT analysis are represented in this figure. The two left-most columns represent the first stage, i.e., the barrier analysis and the two on the right side represent the second one, i.e., the analysis of radiological consequences. In the first column, a particular safety variable in a particular DBT is represented. Since each DBT is an enveloping scenario, the extreme value of the safety variable in the enveloped transients will stay below the value of the same variable in the DBT which should, indeed, stay below the acceptance criterion or safety limit. There will be as many "left-most columns" as the number of safety variables times the number of DBT. This is indicated in Figure 1 by the dashed ellipse entitled "Other S.V. and Acc. Crit." (Other safety variables and acceptance criteria). In every one of these columns there will be an Analytical Margin and a Licensing Margin.

Figure 1. Safety margins in the analysis of Design Basis Transients



Each safety variable and its corresponding safety limit are selected to prevent a particular failure mode of a protection barrier. However, the safety limit is not a sharp boundary between safety and failure. Over-passing the safety limit means that there are non-negligible chances for a given barrier failure mode but, in most cases, there is a margin (the Barrier Margin in Figure 1) between the safety limit and the actual failure. A given failure mode of a particular barrier can result from a variety of transients, as indicated by the converging arrows linking the two first columns of Figure 1.

As in the previous case, there are several possible modes of failure of each barrier, as indicated by the dashed ellipse "Other barrier failures". Each combination of barrier failures and type of accident gives rise to a particular release of radioactive products (source term), as indicated by the converging arrows linking the second and third columns. Again, a limited set of enveloping DBT is selected in order to perform the source term analysis. These DBT will be, in general, fewer and different from those used in the barrier analysis. The selection of DBT for source term analysis and the analysis of these DBT to confirm that they remain below the Source Term Reference Limit introduce two new margins, identified as Source Term Analytical Margin and Source Term Margin in Figure 1.

Finally, the fourth column represents the calculation of radiological effects of the release in terms of doses. The use of the Source Term Margin allows decoupling the dose calculations from the source term analysis. If the doses resulting from a release equal to the Source Term Reference Limit are lower that the Authorized Dose Limit, any change in the source term analysis does not force a recalculation of doses, provided that the new source term remains below the reference limit. The drawback of this approach is that it could result in a more difficult application of the ALARA (As Low As Reasonably Achievable) principles. In any case, the difference between the calculated dose and the Authorized Dose Limit is an additional margin, identified as Dose Margin in Figure 1.

A Global Plant Margin is indicated in Figure 1. However, this is only a qualitative concept. Note that each column of this figure corresponds to different physical magnitudes and, therefore, they cannot simply be summed-up. In addition, we have concurrent margins that cannot be easily combined into a single margin measurement. It is clear that an adequate Global Plant Margin can only be ensured if all the partial margins exist. Moreover, the larger the partial margins, the larger the plant margin. However, a quantification of the Global Plant Margin is not possible.

The difficulty to quantify the Global Plant Margin resulting from the analysis of DBT is not the only limitation of this concept of plant margin. Worldwide experience on the operation of nuclear power plants showed soon that the exclusive use of the analysis of DBT to assess the plant safety could be insufficient. Some events, especially the TMI accident, showed that more complicated scenarios, resulting from out-of-design sequences of events ought to be addressed. The question of how to deal with

so many possibilities made it inevitable to better evaluate their frequencies in order to weight their relative importance. This gave rise to the incorporation of system reliability engineering techniques as it had been advocated by some precursor studies, like WASH-1400 in USA or the Deutsche Risikostudie Kernkraftwerke in Germany. Among other important lessons learned from this experience was that operators and their actions were needed but not necessarily beneficial, so their impact should be taken into account.

Probabilistic Safety Assessment (PSA) techniques implement these new aspects of the safety analysis but they have been applied only to the assessment of severe accidents and their consequences. Other types of accidents, more likely to occur but resulting in lower consequences, are included in PSA «success» sequences and are neither quantified, nor analyzed in detail. As a consequence, the rules on the use of PSA for licensing purposes, when existing, often include a requirement to demonstrate that "enough safety margin is maintained". What is, then, enough safety margin? This question cannot be answered neither with the analysis of DBT only nor with PSA only. The development of integrated methodologies for safety analysis is a necessary condition to adequately address the problem of assessing the sufficiency of safety margins, i.e., the overall level of safety.

In summary, design techniques and traditional licensing practices are oriented to ensure the existence of safety margins in the protection design. However, the question of whether the resulting margins are enough to provide an acceptable level of safety has been only partially solved. The need to better address this question has given rise to some international initiatives.

2. First Pilot applications. CSNI Safety Margin Action Plan (SMAP)

2. First Pilot applications. CSNI Safety Margin Action Plan (SMAP)

The NEA Committee on the Safety of Nuclear Installations (CSNI) promoted in 2003 an Action Plan on Safety Margins (ref. [1] and [2]). A working group was established that developed a framework for integrated assessment of the changes to the overall safety of the plant as a result of simultaneous or cumulative changes in plant operation or design.

While the general objective of SMAP was defined as «To develop guidance on how to assess safety margins in nuclear power plants», three more specific objectives were established in the mandate of the CSNI:

- To agree on a common conceptual framework that, based on both probabilistic and deterministic considerations, could address the safety margin problem.
- To develop guidance on how safety analysis methods and tools can be used to address the safety margin problem.
- To exchange information and experience among the participating organizations.

Experts from 15 countries (Belgium, Canada, Czeck Republic, Finland, France, Germany, Japan, Korea, Mexico, Slovakia, Slovenia, Spain, Sweden, Switzerland, USA) and a representative of the IAEA participated in this working group under the chairmanship of Mr. O. Sandervåg from SKI (Sweeden) with the support of the technical secretariat provided by the NEA and mainly developed by Mr. M. Hrehor.

2.1. Summary of SMAP

One of the key ideas developed in SMAP was that the sufficiency of safety margins cannot be assessed on the basis of a reduced number of design basis accidents. Ideally, any transient challenging some acceptance criterion of the safety analysis should be evaluated. This idea results in the extension of the analysis scope from the traditional *design basis space* to the *risk space* which tries to include any possible transient in the plant. To this aim, the use of PSA techniques such as event trees and fault trees could be convenient. In particular, PSA-like event trees can be useful means to describe the risk space, although this extension is not straightforward.

A set of safety objectives can be defined in terms of limits that should not be exceeded. These safety objectives should include, at least, those limits that were used as acceptance criteria in the traditional

safety analysis of DBT. The plant response for each sequence included in the risk space is then evaluated against the specified limits to determine if some of them are actually exceeded.

For a proper evaluation of the plant response the use of best-estimate simulation models is almost a requirement and for adequate consideration of the plant response variability a comprehensive uncertainty analysis is mandatory.

The SMAP framework therefore results from an effective integration of deterministic and probabilistic methods:

- The design basis space is extended into the risk space, described by PSA-like event trees.
- The PSA sequence success criteria are extended to include a set of selected safety objectives that should include the acceptance criteria used in Design Basis Transient Analysis.
- Risk space sequences are analyzed using a Best Estimate Plus Uncertainty (BEPU) approach, typical of Design Basis Transient Analysis.
- Safety margins for each sequence or, more exactly, lack of them, are evaluated in probabilistic terms.

The final objective is to evaluate exceedance frequencies of the selected safety objectives.

2.2. Probabilistic evaluation of safety margins

Safety margins are most often measured in physical variable units. While this is a convenient approach for design purposes, it makes difficult, if not impossible, the aggregation of existing margins in order to perform an overall margin assessment. Among some possible solutions to homogenize safety margins, a probabilistic definition of margin seems to be the optimal solution. To this aim, some concepts have been borrowed from the *stress-strength* reliability theory.

In a general case, the challenge to some safety objective can be described and quantified by process variables or combinations of them which are called *safety variables*. A safety objective can be described by a probability distribution $f_c(s)$, which is called the *strength* or *capacity* function. This function describes the probability of transition to an undesirable state as a function of the safety variable s. For example, the capacity function of a barrier for a given failure mode describes the failure probability of the barrier as a function of some safety variable, specific of the failure mode.

On the other hand, safety objectives can be challenged as a consequence of the occurrence of undesirable events. The evolution of the safety variables during the subsequent plant transient quantifies those challenges. Usually, the focus of attention is put on the maximum challenge represented by the extreme value (maximum or minimum, depending on the particular case) of the safety variable along the transient. However, the occurrence of a particular event or set of events (i.e., a sequence), does not result always in the same extreme value of the safety variable and therefore on the same level of challenge to the safety objective. Multiple uncertainties in the expected dynamic evolution of the plant make the resulting safety variable value to be a random variable. The probability distribution of this variable, conditional to the occurrence of the specified sequence, is the *stress* or *load* function $f_l(s)$ for that sequence.

The safety objective will be maintained if the load L is less than the capacity C and it will be exceeded if the load L is greater or equal than the capacity C. Therefore, the safety margin associated to a given sequence for a specified safety objective can be measured as the conditional probability of maintaining the safety objective. This probability is given by:

$$p(L < C) = \int_0^\infty f_l(L) \left[\int_L^\infty f_c(C)\, dC \right] dL \tag{2-1}$$

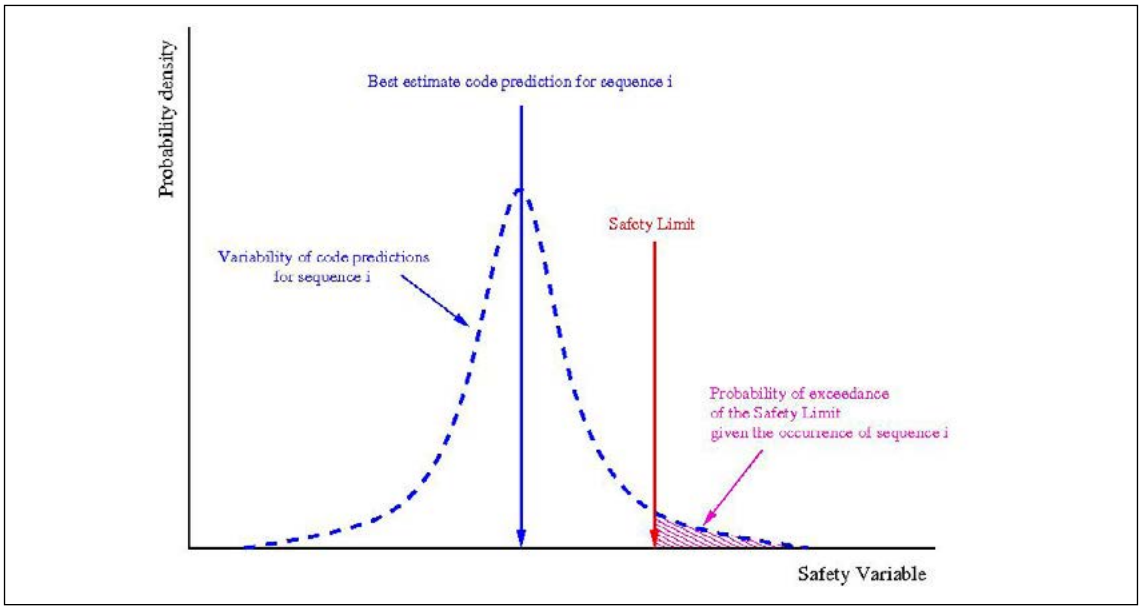
However, the real objective of a safety margin assessment is not to quantify the magnitude of the existing margins but to ensure that they provide an adequate level of safety. For this purpose, quantifying the lack of safety margin, i.e., the exceedance of the safety objective, is much more useful. The conditional exceedance probability of a sequence for a specified safety objective is the complement of the safety margin of eq. (2-1) and can be calculated by another convolution of the load and capacity functions:

$$p(L \geq C) = \int_0^\infty f_c(C) \left[\int_C^\infty f_L(L)\, dL \right] dC \tag{2-2}$$

Equation (2-2) measures the degree of overlapping of the two functions. Exceedance probabilities of all the possible sequences, weighted with the sequence frequency, can be aggregated to calculate the exceedance frequency of the safety objective.

Traditional safety analysis and their associated licensing requirements have been most often based on the use of safety limits. A safety limit L_s is a discrete value of a safety variable that replaces the capacity function $f_c(s)$. This replacement may be accepted from the safety point of view if the safety limit bounds the capacity function on the safe side. In other words, the safety limit will be adequate if the failure probability is negligible (ideally, null) even if the safety variable reaches, but does not exceed, the safety limit.

Figure 2. Exceedance probability in the safety limit approximation



In the safety limit approximation, it is assumed that exceeding the safety limit is already an undesired situation. They become, therefore, surrogate safety objectives and the safety margin assessment can be done on the basis of exceedance frequencies of the safety limits.

Replacing $f_c(s)$ by L_s simplifies eq. (2-2) which becomes:

$$p(L > L_s) = \int_{L_s}^{\infty} f_l(L)\,dL \tag{2-3}$$

which can be easily interpreted in graphical terms as shown in Figure 2.

Most often, the capacity functions describing safety objectives are not easily available. Instead, safety limits can be taken from deterministic safety analysis and significantly simplify the calculations. Therefore, the safety limit approximation can be expected as the most usual approach, even for safety margin assessment studies.

2.3. Main results of SMAP

The SMAP group issued several Technical Notes as working documents (ref. [1]) and a Final Report (ref. [3]) that was published in 2007. These documents provide guidance on how to address the assessment of changes in safety margins due to significant plant modifications. The contents of the Final Report is summarized below:

- Chapter 1 provides a discussion on the safety margin issue, existing related concepts and the needs of the stakeholders.
- The different contributors to the global plant margin and the definition of proper terminology are described in Chapter 2 that also includes a short description of existing systems of safety and acceptance limits.
- Chapter 3 discusses the assessment process of the safety margin quantification. It first develops the conceptual model in the risk space and then proceeds to characterize transient analysis tools and the possible modes of application to safety analysis. In a second step, uncertainties are classified and some guidelines are given for specific treatment of different uncertainties in the quantification process.
- The link between physical damage limits and the risk space via the load-strength concept is established in Chapter 4.
- Chapter 5 describes the general concept to quantify plant safety margin and ways of aggregating the risk contribution for different event sequences.
- Finally, pilot applications of the methodology are documented in Chapter 6.

The main results and conclusions of the SMAP activities, as documented in the final report, were:

- The proposed framework provides adequate means for estimating the effect of a broad range of plant modifications.
- SMAP integrates existing methodologies for safety margins and risk evaluations. The resulting risk indicators include consideration of safety margins.
- Risk indicators are given as expected frequencies of specified plant damage states (limit exceedance frequencies)
- The proposed approach is able to merge information from all the relevant disciplines in regulatory decision-making (plant simulations, probabilistic analysis, material science and

engineering, etc.). The integration can be done with existing, tested tools and methods. Yet, the integrated framework has the potential to evolve as new tools and methods will become available.

With regard to the development of specialized tools, it was stressed that availability of dynamic event tree simulation tools would be advantageous for an efficient application of the SMAP framework. Among the recommendations included in the report, it was suggested to launch an international exercise for exploring the performance of different approaches for this type of tools. So far, no such exercise has been formally proposed within the CSNI. However, the subject has evolved in other forums as will be discussed in section 4 below. In addition, the dynamic event tree method showed its applicability in SM2A, a follow-up exercise developed as a first application of SMAP (see Section 3).

2.4. CSN MOSI participation at the SMAP Group

For participation in SMAP, CSN nominated a delegate belonging to the department of Modeling and Simulation (MOSI). He developed an intense activity in the group, particularly convincing other participants of the need to incorporate PSA integrated techniques to address the safety margin assessment issue. He actively participated in the elaboration of several Technical Notes issued as partial activity reports and was a member of the writing group that produced the draft of the final report [2].

3. First Pilot applications. The follow-up of SMAP: the SM2A exercise

3. First Pilot applications. The follow-up of SMAP: the SM2A exercise

Once the SMAP task was completed, an application exercise was also promoted by the CSNI and a follow-up task group was formed under the name of Safety Margin Assessment Application (SM2A). The focus of this exercise was the assessment of the practicability of the SMAP framework. The activities of this group started in January 2008 and the final report [3] was published in 2011.

The initial mandate of the CSNI in June 2007 was to apply the SMAP framework for the assessment of changes in safety margins that could result from the application of the newly proposed alternative LOCA rulemaking of the USNRC. Consistently with this mandate, the task group was initially named LOca Safety MArgins (LOSMA)

The expected outcome would be an appraisal of the SMAP framework by estimating the effect of physical or operational changes in safety margins. According to the mandate, preliminary results should be made available to CSNI by June 2009.

The group was formed by experts from 10 countries (Czech Republic, Finland, France, Germany, Japan, Korea, Mexico, Spain, Switzerland and USA), all of them former participants in SMAP although in some cases the participating organizations were different. As in SMAP, a representative of the IAEA was also participating as an observer. The Technical Secretariat was mainly developed by Mr. A. Amri (OECD/NEA) and the group was chaired by Mr. M. Zimmermann from PSI (Switzerland). In addition, the CSNI required close collaboration with the Working Groups on Accident Management and Analysis (WGAMA) and Risk Assessment (WGRISK). To better implement this collaboration, two experts from WGRISK joined the group from the second meeting and two participants in WGAMA from the Pisa University attended also the 3rd and 4th meetings.

The mandate of the CSNI was deeply discussed in the first meeting of the task group. It was considered that including the proposed LOCA rulemaking in the name of the group would indicate possible regulatory implications that were not found appropriate for a research group. In addition, it was also concluded that a change in rulemaking can only have an indirect impact on the safety margins of any nuclear power plant. The change in the rulemaking, by itself, does not impact any safety margin. Only changes that are actually implemented in the plant, some of them made possible only after a change in rulemaking, could impact the safety margins.

Based on the above considerations, it was decided to change the proposed name of the group to Safety Margin Assessment Application (SM2A) which better describes the purpose of the group. The scope of the application exercise was also extensively discussed and it was decided to apply the SMAP framework

to the analysis of a hypothetical power uprate in a typical PWR nuclear power plant. Power uprates are among the significant changes in nuclear power plants prone to impact a variety of safety margins. Moreover, it can be expected that some plants could not be allowed to implement a significant power uprate unless some rules (such as the LOCA rule) are previously changed.

A 10% power increase was considered a good choice for the pilot application. On the one hand, it is high enough as to produce a broad impact on the plant systems and operations. On the other, it is low enough as to not requiring strong changes in the analysis tools and models as a consequence of the plant changes.

The Zion plant was selected as the reference for the application exercise. It is a Westinghouse 4-loop PWR plant which is in permanent shutdown. This was a main reason for the choice because, being a non-operating plant, any conclusion that could be drawn from the results of the exercise would have no licensing implications. In addition, most, if not all, the participants had simulation models of Zion, at least at the LOCA analysis level, since this plant has also been used in other international exercises such as BEMUSE. Finally, Zion was also one of the reference plants for the PSA pilot application documented in NUREG-1150. Therefore, a PSA model for Zion was also publicly available, although the documentation that could be accessed was far from detailed.

3.1. Adaptation of the SMAP framework to SM2A

Being SM2A the first large scale application of SMAP, some adaptation of the general framework was needed. Some propositions of SMAP, for example, were formulated in a rather general way and needed some more development for a practical application. In other cases the general framework offers different options and one of them must be selected. Finally, the specific constraints of the SM2A mandate imposed some restrictions and simplifications in the application.

The main adaptations of the framework that were implemented for the development of SM2A were the following:

- Use of a bounding safety limit instead of the barrier strength function

As indicated in Sectio n 2.2 above, this approximation is expected to be the most usual option for the calculation of conditional exceedance probabilities in safety margin studies.

- Selection of Peak Clad Temperature (PCT) as the only safety variable for analysis

In Secti on 2.1, it was said that a complete safety margin assessment should consider as safety objectives at least those limits used as acceptance criteria in the traditional safety analysis. This is an adequate way to get a good coverage of the whole range of risks including from low damage / high frequency scenarios up to high damage / low frequency ones.

To this aim, it was initially proposed that SM2A should include at least the analysis of two safety limits, namely PCT < 1204 ºC and DNBR > 1.3, as representatives of two separate areas of risk. However, even this reduced scope of the analysis could not be finally applied, mainly because of two reasons: the lack of a PSA-like model for the DNBR limit and the strong time limitation of SM2A as per mandate. Consequently, only the PCT limit was finally analyzed.

In a real safety margin assessment this would be an unacceptable simplification. However, the main objective of SM2A was not to get a conclusion on the acceptability of the power uprate but to show how to apply the safety margin methodology. Although the analysis of other limits could introduce some specificity in the methodology, the limitation of SM2A to a single safety objective was not considered a serious drawback for a first appraisal of the SMAP framework.

- Reliability models: some cases were analyzed at PSA sequence level

Fault trees are used both in PSA and safety margin assessments. However, there could be important differences between the types of fault trees needed in each case. For PSA, fault tree models represent minimal system configurations needed to achieve successful safety functions. Instead, safety margin assessments need to model any possible configuration of the safety systems, regardless of previous considerations on the ability to perform the required safety function.

In principle, PSA fault trees are not directly usable for safety margin assessment studies. However, it can be expected that adequate fault trees could be obtained by rearranging the PSA fault trees, possibly with a few additional changes. In particular, operator actions in safety margin studies are a part of the uncertainty analysis (time uncertainty) and should be taken out of the fault tree models where they are represented only by a failure probability based on the concept of available time.

Any modification or rearrangement of PSA fault trees requires a good knowledge of the original model. This was not the case with the Zion PSA. The lack of detail in the available documentation made in many cases impossible modeling the different configurations of the safety systems. As a consequence,

most of the SM2A analysis was performed by considering only the PSA configurations, i.e., minimal configuration for success or total failure.

- Treatment of uncertainties: SM2A calculations did not separate uncertainties by type

The need to separate aleatory (intrinsic variability of events and phenomena) and epistemic (lack of knowledge) uncertainties has been and continues to be discussed for a long time in the open literature. Some authors think that the different nature of these uncertainties should result in a different treatment for each one. According to these authors, a proper separation is a requirement for supporting risk-informed decision making. Otherwise, the results of the uncertainty analysis could be difficult to interpret, misleading or even wrong. Separation of uncertainties was recommended in the SMAP report (ref. [2]), noting that it implies a nested two-loop calculation scheme.

Other authors, instead, believe that such a distinction is not needed and that whatever the uncertainty type is (epistemic or aleatory), uncertainty is in any case a question of degree of belief.

When applied to the calculation of exceedance frequencies, the separation between aleatory and epistemic uncertainties makes the resulting exceedance frequency being a random variable. The exceedance frequency values carry the information coming from the aleatory uncertainty while the distribution of the variable shows the effect of the epistemic uncertainty. If the separation is not performed, the result is a discrete value corresponding to the mean value of the random variable (expected value of the exceedance frequency).

The SM2A calculations did not separate between the two types of uncertainties. The task group agreed that implementing the two-loop treatment of uncertainties exceeded the resources available for the exercise by a large margin. In addition, because the simulated plant response is comparable in the reference and the up-rated cases and the same epistemic uncertainties apply to both, the impact of not distinguishing between the types of uncertainties is minimized when evaluating a CDF change (i.e., delta-CDF). The reason is that, being the exceedance frequencies before and after the change highly correlated random variables, their difference will show much less uncertainty than each separate variable. Under these conditions, the difference of the mean values can be taken as a good estimation of the exceedance frequency increment. On the contrary, if an absolute CDF estimation needs to be compared with an acceptance criterion, explicit separation between aleatory and epistemic uncertainties may be unavoidable.

3.2. Development of the SM2A exercise

Following the general SMAP procedure, the main steps in the development of SM2A can be summarized as follows:

1. **Define the power uprate method.** Among the different options to increase the power in the reactor core, it was decided to flatten the radial power distribution while maintaining the power of the hottest element in the core. Coolant flow and cold leg temperature would remain at their nominal values for the initial state. This option was considered the one that minimizes the impact of the change on the simulation models.

2. **Take the Zion PSA event trees as an initial description of the Risk Space.** In classical PSA the term «core damage» indicates transition to severe accident conditions. This transition is defined by several conditions, a main one being the exceedance of the PCT limit. Therefore, both classical PSA level 1 and SM2A focus on the same limit. This makes the set of PSA event trees to be a good starting point to define the Risk Space for the SM2A exercise.

3. **Review Zion event trees to identify sequences potentially more affected by the power uprate.** In order to minimize the number of calculations it is very convenient to first perform a qualitative analysis, possibly supported by simplified quantifications. The objective is to identify a first set of sequences as candidates for detailed analysis. It should be noted that the sequences more affected by the change are not necessarily the PSA dominant sequences. On the contrary, it can be expected that the most sensitive sequences are those located near the border between success and core damage, with little or null contribution to the core damage frequency in the initial plant state.

4. **Discard sequences of very low frequency.** Broadly speaking, the contribution of a sequence to the limit exceedance frequency is a fraction (between 0 and 1) of the sequence frequency as calculated in PSA. Therefore, very low frequency sequences can be excluded from the safety margin analysis because they cannot give significant contributions to the exceedance frequency. However, this exclusion must be done very carefully. It must be checked that not only the individual frequencies of the excluded sequences but also their collective frequency are negligible. For SM2A, an arbitrary cut-off value of 10-7 was selected as screening threshold. This value would be too high for a real assessment of safety margins but the constraints of the SM2A mandate required a strong reduction in the number of sequences to be analyzed in detail.

5. **Refine PSA sequences to get non-ambiguous simulation scenarios.** As indicated before, the possible states of a safety system in PSA are grouped only under two configurations, namely, minimal configuration for success or total failure. This is acceptable in the PSA context where

the focus is on frequency quantification. However, different success configurations or different failure configurations could result in different consequences. Moreover, when simulating the plant dynamics, the configuration of every system must be well specified. It is not possible to run a transient where «two or more» trains of a system are available. When possible, the Zion PSA sequences have been split in different system configurations. Unfortunately, in most cases the analysis was restricted to minimal configuration and total failure.

6. **Calculate conditional exceedance probabilities using BEPU methods.** For each sequence of interest, the conditional exceedance probability is calculated by using best estimate simulation codes and applying uncertainty analysis methods. The contribution of each sequence to the limit exceedance frequency is the product of the sequence frequency by the conditional exceedance probability.

Given the limitations in the number of participating organizations and available time, not all the Zion event trees were analyzed. Some of them were discarded with the assumption that they were not too sensitive to the power uprate. The remaining event trees were distributed among the participants. Although the general criterion was to assign an event tree for each participant, some organizations analyzed two event trees with similar characteristics and some event trees were analyzed by two collaborating organizations.

All the event trees were analyzed following the SMAP principles. However, not all the analyses were done following exactly the same procedure. Since the main objective was to assess the analysis methods, not to get a meaningful result, each participant was allowed to choose its own simulation tools and its own method for uncertainty analysis. Even though all of them could be considered BEPU applications, the results obtained by the participants were not homogeneous and the task group decided not to aggregate the results to give a final result. This was not considered an important drawback for an application exercise where no decision should be taken on the basis of this result. The advantage is that it has been shown that the SMAP framework is very flexible and can be adapted to different application environments.

Table 1 shows the event tree assignments, the number of sequences initially selected for detailed analysis and the results obtained by each participant. The final number of analyzed sequences is actually greater than the one indicated in Table 1 because, on the one hand, the conditional exceedance probability of some sequences can be set to 1 from a qualitative analysis, and on the other, some non-selected sequences became analyzed as a by-product of the analysis of a selected sequence. The latter occurs, for example, when a safety function occurs at uncertain time: analyzing the case of safety function success but delaying the time of intervention makes the sequence slowly moving to another sequence with the safety function failed.

Table 1. Overview of Impact on PCT exceedance frequency and its increment by scenario

Scenario (Note 1)	Organization	No. of selected sequences	Ex. Freq.(y^{-1}) 100% power	Ex. Freq.(y^{-1}) 110% power	Ex.Freq.(y^{-1}) Increment
Loss of Offsite Power + Loss of FW	CNSNS, IRSN	1	2.81E-06	3.29E-06	4.8E-07
Loss of SW and/or CCW	CSN	1	1.34E-06	1.46E-06	1.18E-07
MBLOCA	PSI	2	8,39E-07	1,64E-06	8.01E-07
Loss of Offsite Power + Seal LOCA	CNSNS, IRSN	1	(Note 2)	(Note 2)	<< 1.0E-07
Steam Line Break + Loss of FW	STUK, GRS	1	(Note 3)	(Note 3)	<< 1.0E-07
LBLOCA	EDF, NRI	4	2.49E-09	2.52E-09	2.8E-11
SBLOCA	PSI	1	(Note 2)	(Note 2)	<< 1.0E-07
Turbine Trip	JNES	5	0.0	0.0	0.0
Loss of Main Feedwater	NRC	2	0.0	0.0	0.0
SGTR	KAERI, KINS	3	9.3E-10	9.3E-10	0.0

Notes to Table 1:

1. Acronyms used for the scenario identification:
   FW: Feed Water.
   SW: Service Water.
   CCW: Component Cooling Water.
   LOCA: Loss of Coolant Accident.
   LBLOCA: Large Break LOCA.
   MBLOCA: Medium Break LOCA.
   SBLOCA: Small Break LOCA.
   SGTR: Steam Generator Tube Rupture.
2. The scenario was found little sensitive to the power uprate. The exceedance frequency increment was estimated very low and no uncertainty analysis was done.
3. Only a very low frequency scenario (4.35E-11 y^{-1}) showed sensitivity to the power uprate. The exceedance frequency increment was estimated very low and no uncertainty analysis was done.

Detailed results were provided by each participant and reported in appendices of the final report of SM2A. A summary of the analysis and results reported by the CSN for Loss of SW/CCW, is presented later in Section 5.

3.3. Lessons learned and conclusions from SM2A

From the first large-scale application of the SMAP framework, the task group learned some important lessons that should be taken into account for future applications.

Setting-up a well prepared set of analysts to perform the job is the first key for success. From a quick look to the SMAP steps it could be concluded that sequence selection is an initial step, mostly based on PSA techniques, while transient simulation is a subsequent step. However, the SM2A experience showed that a very close interaction between different experts is needed from the very beginning. Transient simulation expertise is essential for a good selection of sequences and probabilistic expertise is also important in the transient simulation phase, both to a much greater degree than initially expected. The consequence is that a combined team with both types of experts, able to understand each other and maintaining a continuous interaction is much more adequate for developing safety margin assessment studies than two separate teams, even if they interact in a regular but non-continuous way.

The risk space is described by a large set (hundreds or, may be, thousands) of sequences. Depending on the particular problem, the sequences that need to be analyzed are different. If the absolute level of safety is being assessed, probably most of the sequences need to be evaluated. Even in this case, an initial selection of the most significant ones could be very helpful for a successful end.

When the object of the analysis is a plant change potentially impacting safety margins, sequence screening is even more important since not all the sequences of the risk space are equally sensitive to the change. In the case of SM2A it was found that only a limited set of sequences had to be analyzed in detail. Even though the case of SM2A is not totally representative, given the high value of the frequency cut-off for sequence filtering, there is an important message behind: an efficient screening of sequences is a key for success in safety margin assessments. Failing to perform such a screening would result in an unacceptably high number of simulations, many of them just showing no impact from the plant change.

In the screening process, it is worth to note that the most sensitive sequences are not, in the general case, the most contributive ones to exceedance frequencies before the change. A plant change may impact the frequency of a sequence, its conditional exceedance probability or both. Dominant sequences in any plant state are usually sequences where the conditional exceedance probability takes values close or equal to 1. Therefore, the effect of a plant change on initially dominant sequences tends to concentrate on the sequence frequency only. This makes dominant sequences less sensitive than sequences with small but non-negligible values of conditional exceedance probability.

In addition, a screening process based on the evaluation of a single typical transient per sequence could be misleading. While a typical or best estimate transient could lead to a successful end state, the sequence could still give a non-negligible contribution to exceedance frequency when considering the variability of uncertain elements.

Looking at the results of SM2A it can be observed that the most contributive sequences to the increase in exceedance frequency involved uncertain time delays associated to manual actions or recovery

of failed safety functions. This result suggests that sequences containing uncertain time delays, i.e., stochastic events, are clear candidates for detailed analysis.

A side implication of this finding is that probability distributions of time delays are very important. However, in many cases these distributions are almost unknown. The scarcity of measured data makes it necessary to relay on assumptions and approximations that could strongly condition the results.

Among the precautions that should be taken into account when approximating delay distributions, SM2A showed that the use of no-tail functions (such as uniform or triangular) can be misleading. Limit exceedance is more likely for long delays and this compensates the low probability associated to distribution tails. The net result is that shortening the tail of the distribution may hide the problem and give a false null contribution to the exceedance frequency.

As a main conclusion from the exercise, the task group considered that the SMAP framework has been shown technically feasible in terms of its capability to evaluate changes to safety margins as a result of cumulated or complex plant/operating modifications. Nevertheless, it should not be forgotten that SM2A was but a pilot study. Several areas of improvement were identified, mostly related with some of the lessons learned. Whether the effort of developing these improvements is compensated by the added value of safety margin studies is still to be determined.

3.4. MOSI/CSN participation and lessons learned as a result of the SM2A

As indicated in table 1, MOSI participated actively in the analysis of one of the scenarios and in the writing of the final document of ref. [3]. In addition to contributing to the international objective, MOSI used the opportunity to develop a roadmap for ISA. Performing a first application of the methodology, even with the constraints imposed by the exercise, allowed for identifying areas of interest in order to further advance the licensing approach based on specific checks of industry safety assessments, as detailed in ref. [13]. Among the focus of activities, the ISA application to the verification of emergency procedures and the consistent use of the results of the fault tree event tree models of our plants were of primary interest.

The details of the contribution of CSN-MOSI to SM2A, consisting of the analysis of the loss of CCW/SW systems scenario, will be given in Section 5 of this report.

One new aspect, specific of the integrated methods, is the importance of separating the transients within a sequence in two groups: transients ending or not in sequence failure, i.e., in safety limit

exceedance. Only failed transients are relevant for exceedance frequency quantification but in a well protected facility they are expected to be much less than the safe transients. In addition, for a transient to be given credit, no action or phenomenon may occur without activation of the corresponding stimulus, i.e., alarms or procedure entry conditions for manual actions, initiation setpoints for automatic actions and required conditions for phenomena not linked to intended actions.

The timing of the events, including activation events, is then of primary importance in the process of discriminating failed from safe transients. As a result time uncertainty techniques become essential although they are not included as such in classical uncertainty techniques. Due to this, a specific ISA time uncertainty method has been developed by MOSI in the course of the SM2A exercise and is described in Appendix A.

4. Present Status of Integrated Methods and SM applications

4. Present Status of Integrated Methods and SM applications

Following the completion of the SM2A exercise, international activities have evolved in two directions. One is the development of integrated PSA/DSA methods (IDPSA) intended for a variety of nuclear safety applications and the other is the development of specific methods for characterization of safety margins (SM). These two directions, however, are not diverging very much since IDPSA methods still are usable also for safety margin characterization.

4.1. MOSI/ CSN Proposal: Integrated Safety Assessment methodology

MOSI has followed IDPSA activities as reported in references [4], [5], [6] and [7]. It has been observed that, almost independently of the specific purpose, all the IDPSA developments are following a very similar approach. The specific focus of MOSI activities is the development of tools and methods providing support to licensing activities performed from the regulatory side.

Historically, safety analyses supporting nuclear power plant licensing applications have been closely linked to computational tools, most of them related with simulation of transients and accidents and probabilistic quantifications. Quality and level of detail of this type of tools is continuously increasing and new licensing issues and methods, exemplified by the increasing trend to the so-called Risk-Informed Regulation (RIR) have further motivated new developments in this field.

In addition, the almost continuous improving process of existing plants, the development of new plant designs and the extension of plant licenses to cover longer life times, higher fuel burn-up or increased power levels, among others, represent new challenges that need to be supported by calculations. All these developments require a considerable level of resources.

In parallel, regulatory bodies need to increase their expertise and capabilities in this area. Technical Support Organizations (TSO) have become essential elements of the regulatory process[1], also relying to a great extent on the use of computerized analytical methods and tools.

Regulator and TSO tasks cannot have the same scope of their industry counterparts, nor is it reasonable to expect the same level of resources. Their specific aim is to review and approve methods and results of licensees and to perform their own checks, analyses or calculations to verify the quality, consistency and

[1] Examples of TSOs are GRS, IRSN, PSI and Studvik, which support the regulatory bodies of Germany, France, Switzerland and Sweden, respectively. In other cases, as the USNRC or CSN, regulatory bodies have their own technical staff acting as TSO.

conclusions of industry assessments. This is a very special regulatory task requiring specific diagnostic tools to independently check the validity and consistency of the many assumptions used by the licensees.

The approach and the tools shall include a sound combination of deterministic and probabilistic single checks that, when taken all together, constitute a comprehensive sample for ensuring that the analysis ingredients are properly and consistently weighted and the decision making process is properly supported. The MOSI department of CSN has promoted and developed from CSN such an approach to regulatory computational support which has been baptized as the Integrated Safety Assessment (ISA) methodology, based on the Theory of Stimulated Dynamics (TSD) also developed by MOSI [19].

An integrated view of safety analysis is essential to clarify the relative roles of deterministic and probabilistic types of analysis with a view towards their harmonization. The aim is to take benefit of their strengths and to get rid of identified shortcomings, normally related with inter-phase aspects. Issues such as PSA success criteria or operating technical specifications are among those where interphases between deterministic and probabilistic aspects of the analysis may become critical.

A sound theoretical approach (see ref. [13] and [14]) is at the basis of the ISA method which, in addition, requires a set of computational tools for its application. A suitable software package called SCAIS has been also developed to this aim. Its main feature consists of coupling the following elements (ref. [12], [13] and [15]):

- simulation of accident sequences resulting from exploring potential equipment degradations following an initiating event (i.e., simulation of thermal hydraulics, severe accident phenomenology and fission product transport);
- simulation of operating procedures and severe accident management guidelines;
- automatic delineation (with no a-priori assumptions) of event and phenomena trees;
- probabilistic quantification of fault trees and sequences; and
- integration and statistic treatment of risk metrics.

The ISA approach relies on the concept of Deterministic Dynamic Event Tree (DDET) consisting of the systematic generation of tree structured simulation paths describing possible evolutions of the plant state from given initial conditions and initiating event. Accordingly, among the different modules that compose the SCAIS system, special mention should be given to the simulation driver, called BABIECA, and the event scheduler, called DENDROS. These modules take the main role in the generation of DDETs as illustrated in figure 3. See ref. [13] for more details.

A deeper discussion on the need for development of integrated tools and the required features of these tools can be found also in ref. [13].

New developments and improvements of MOSI methods after participation in SM2A have been documented in detail in ref. [14], where a prototype for experimental implementation and testing of the most recent developments is described. The SCAIS deterministic computer platform and advanced ISA probabilistic prototype are summarized in figures 3, 4 and 5.

A distinctive feature of SCAIS is the extensive use of coupled codes. This has led to the definition and development of a Standard Software Platform (ref. [15]) that allows a given code to be incorporated quickly into the overall system while overcoming difficulties derived from particular models and computational methods.

Applications oriented to verification of Accident Management Guidelines have led to the development of SIMPROC Operator Actions Simulator coupled to SCAIS (figure 4).

Figure 3. Overall BABIECA-DENDROS-Probability calculator coordination

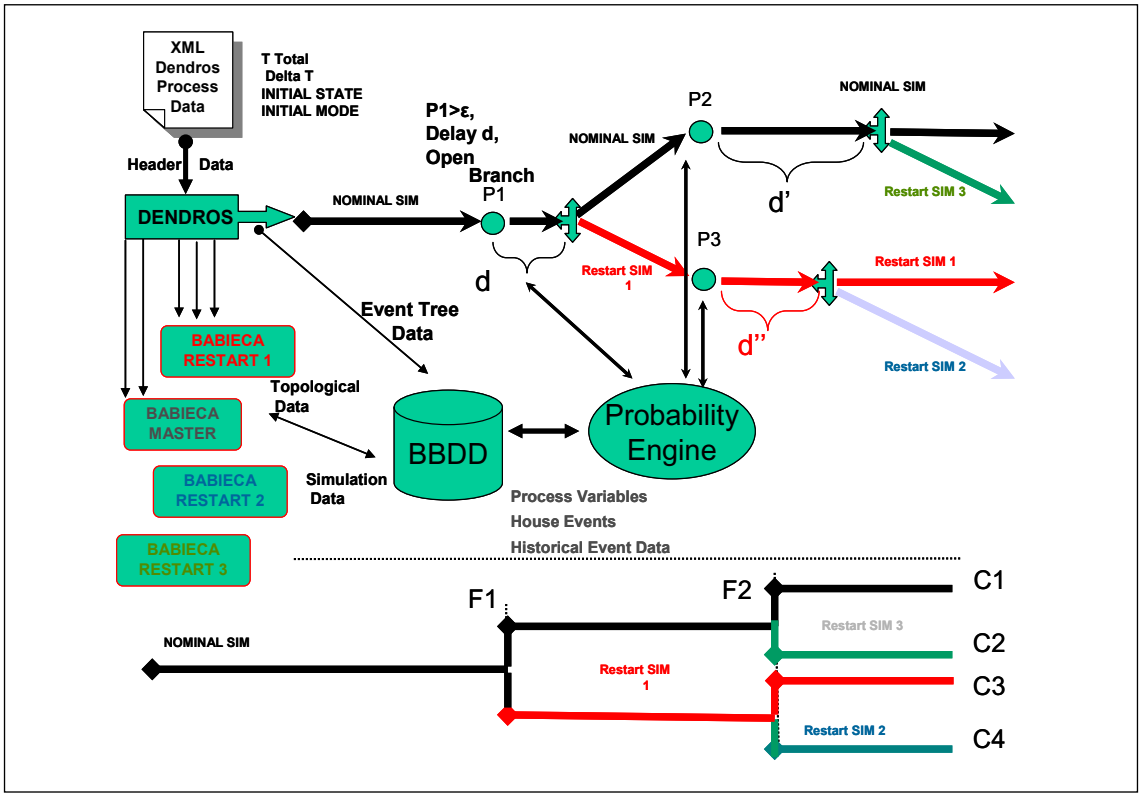


Figure 4. Scheme of SCAIS framework: Simulation of Plant and Operator Actions

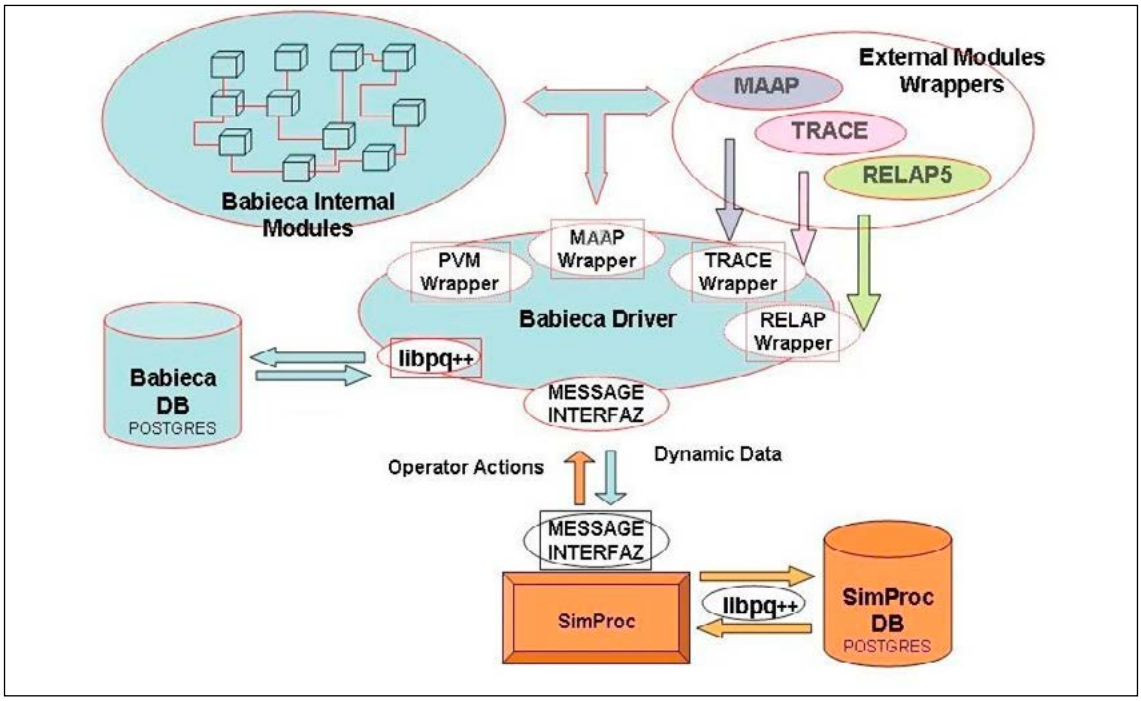
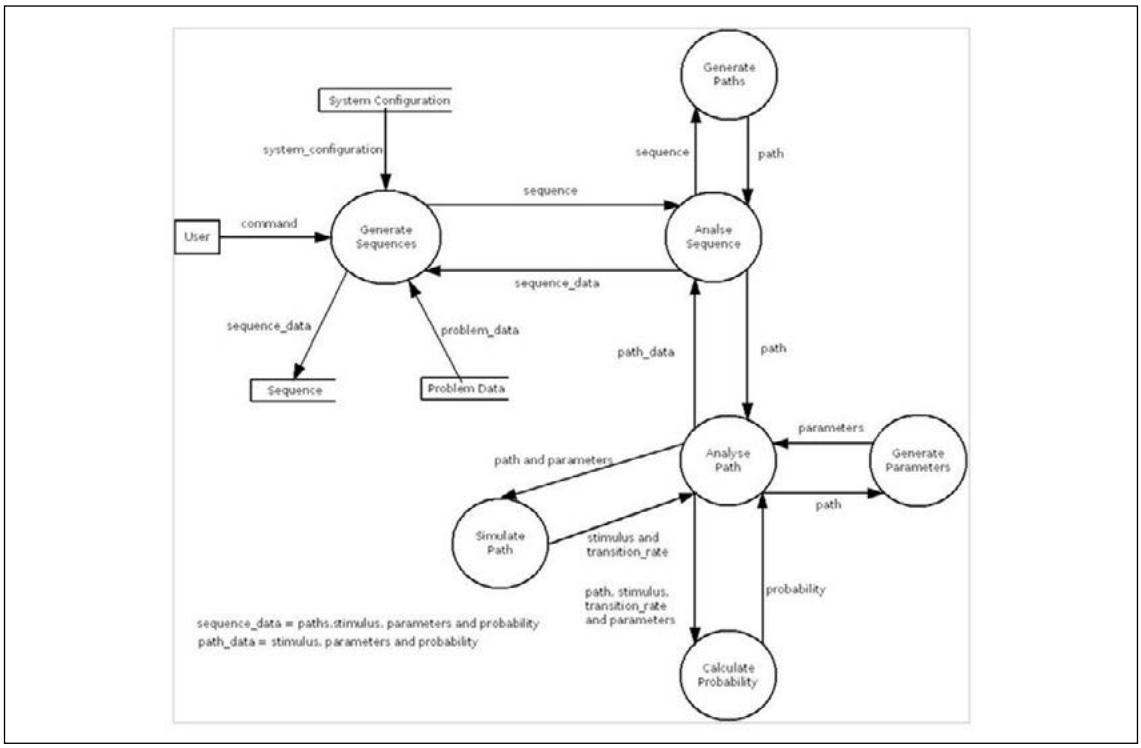


Figure 5. Structural block diagram of TSD prototype



The purpose of the prototype of Figure 5 is to perform the developmental assessment of new modules and algorithms, especially for the search of damage/failure domains and the computation of the exceedance frequency. This way, each research item can be tested off-line before its integration in SCAIS.

4.2. Specific developments for characterization of safety margins

Concerning SM and to show only a recent development and its similarity to the ISA/SCAIS ideas and concepts, we present here the current activity being developed at the Idaho National Engineering Laboratory (INEL) in the USA (ref. [8] and [9]). These developments are being promoted by EPRI (see ref. [10] and [11]), and aim at building and implementing tools and methods that permit cost-effective safety margin assessments, capable of addressing the challenges and opportunities associated with extended NPP operation (i.e., extended plant life cycles). Nevertheless, applications of the approach are not oriented solely to addressing issues associated with ageing management, but also to evaluate opportunities for an enhanced operation.

Figures 6 and 7 show the overall outline of the RISMC (Risk Informed Safety Margin characterization) and Raven toolkit, with components that parallel the structure of ISA-SCAIS framework (see figures 3, 4 and 5, and ref. [12] and [13]). Note that the use of surrogate models of the large codes within the «Simulate Path» block, as indicated in ISA ref. [14], is always necessary.

Figure 6. Scheme of RAVEN framework components

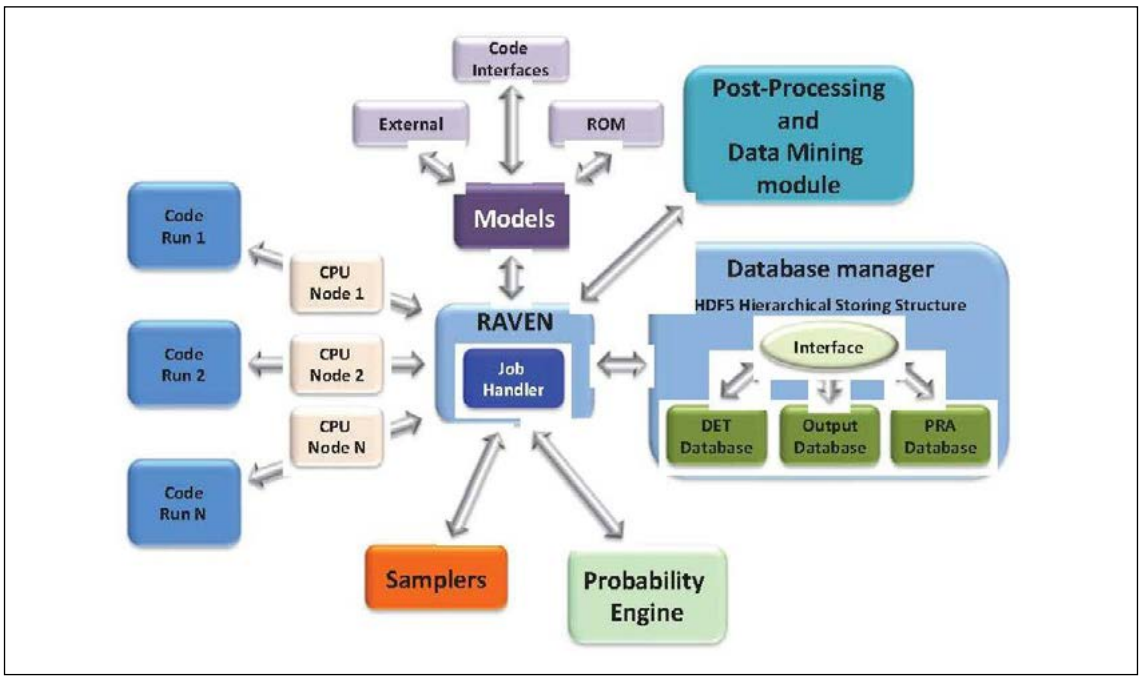
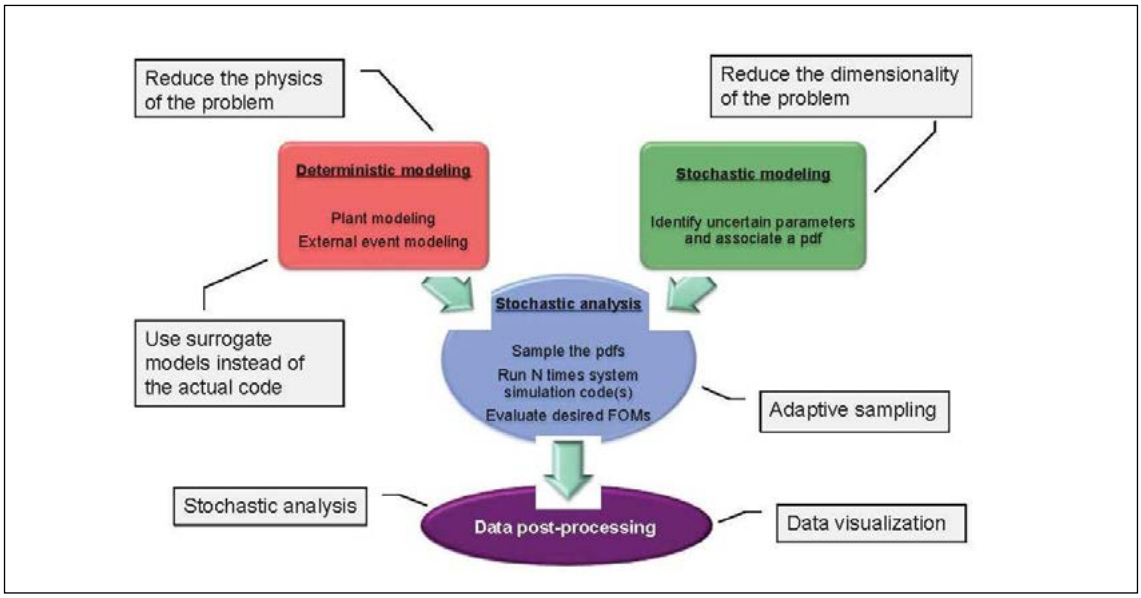


Figure 7. Overview of techniques applied to the 4 main steps of a typical RISMC analysis



It should be noted that the purpose of each organization is very different. MOSI has a very narrow scope of applications, mostly aiming at developing checking tools to be used on a V&V process of specific points in Licensing Safety cases and conformed within CSN needs.

5. SM2A exercise. CSN analysis of the Loss of Component Cooling Water scenario

5. SM2A exercise. CSN analysis of the Loss of Component Cooling Water scenario

The contribution of CSN to the SM2A exercise focused on the analysis of the loss of Component Cooling and/or Service Water scenarios[1] (ref. [3] and [16]).

5.1. Description of the scenario

Loss of Component Cooling Water (CCW) or Service Water (SW) impacts the plant operation due to the loss of cooling of essential equipment, most notably, reactor coolant pumps and safety systems. These two types of scenarios have many common characteristics. SW is a support system for CCW. Therefore, when SW is lost, one of the consequences is the loss of CCW, although there are also some additional effects. Most notably, SW provides cooling water to emergency diesel generators which become unavailable in loss of SW scenarios but not in loss of CCW due to other causes. Also, some containment systems like fan coolers can be affected by loss of SW but not by loss of CCW.

The application in SM2A of a very high cut-off frequency, as described in section 2.1.2, resulted in the practical elimination of scenarios with loss of external power supply since they have a relatively low frequency in the Zion PSA. This made diesel generators irrelevant for our example. On the other hand, since SM2A was exclusively oriented to the exceedance of a fuel limit, the containment safeguards did not play any essential role in the prevention of the core damage. As a consequence, loss of CCW and loss of SW were considered as a single initiator whose frequency, 1.88E-03 y^{-1}, is the total frequency of both initiators in the Zion PSA.

The prevention/mitigation of the consequences of the loss of CCW/SW accidents is dominated by operator actions. An adequate modeling of the scenario can only be done if the actions that the operator is required to execute are known. However, we did not have access to the operating procedures of Zion. Operating procedures of other Westinghouse plants may be a reference although precautions should be taken due to possible significant differences with respect to Zion. Our main references for required operator actions in loss of CCW scenarios were the emergency procedures of Spanish Westinghouse 3-loop plants with a configuration of auxiliary water systems similar to that of Zion.

Upon the loss of CCW/SW, the reactor coolant pumps are the components first affected by the loss of cooling. According to the operating procedures, the high temperature alarm in reactor coolant pumps is the triggering criterion for the operator to trip the reactor and stop the pumps. At the same time

[1] The work was part of the collaboration between Universidad Politécnica de Madrid (UPM), NFQ S.L. (Indizen Technologies) and CSN.

that the main pumps become overheated, other equipment is affected. In particular, charging pumps may result inoperable because of high temperature. Among the important functions of charging pumps we can mention reactor coolant pump seal injection or primary coolant inventory control.

Even if the reactor coolant pumps are stopped, lack of water injection to the seals combined with loss of cooling water to the pump thermal barrier may lead to seal damage resulting in a seal LOCA, a particular case of small or intermediate LOCA, conditioned by the loss of equipment resulting from the loss of the support system CCW. In the Zion PSA this is the greatest contributor to the conditional probability of severe core damage in loss of CCW/SW events. Quantifying the probability of seal failure is not an easy task but a documental review of seal failure models suggests that the 0.73 value used in the Zion PSA may be highly overestimated. A new model was suggested, as discussed below.

The Auxiliary Feedwater System (AFW) plays a very important role in this kind of scenarios. It provides the means for cooling down the plant and guarantees that severe core damage is prevented if the seal LOCA does not occur, even if CCW/SW systems are not recovered. Moreover, cooldown through the secondary system may help preventing the pump seals from failing. This method of cooldown requires not only the AFW system operation but also the opening of a relief or safety valve in those steam generators fed by AFW. Alternative cooling based on reactor coolant system feed and bleed requires CCW recovery since, otherwise, the injection pumps would not be operative.

In the case that a seal LOCA occurs as a consequence of the loss of CCW, safety injection systems (SIS) are needed to compensate the loss of inventory. However, both High Pressure and Low Pressure Safety Injection (HPSI and LPSI) are unavailable while CCW is not recovered. Accumulators are the only available injection system under these circumstances. Surprisingly, the only SIS header included in the Zion even trees for loss of CCW/SW is High Pressure Injection / Feed & Bleed. In our study, all the SIS have been considered, conditioned to the CCW recovery and with their corresponding failure probabilities.

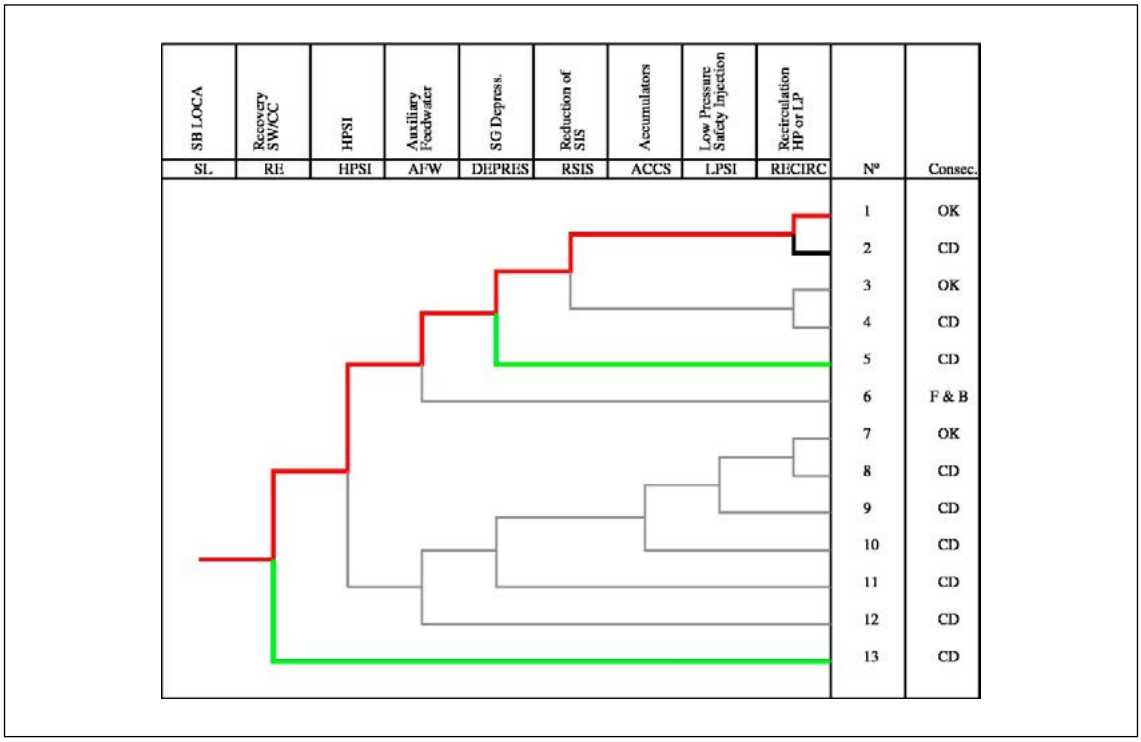
5.2. Sequence screening

A preliminary screening of the loss of CCW sequences was performed, based on the conditional probabilities of the events modeled in the Zion PSA. It was first decided not to consider sequences with reactor trip failure. In the Zion PSA, such sequences are transferred to the ATWS event tree and they should be analyzed there. In any case their contribution can be expected very low. The analysis of ATWS in Zion identifies (Table 4.4.142 of ref. [17]) the dominant contributors to core damage with frequencies ranging from 1.1E-03 to 3.3E-07 and no sequence coming from the loss of CCW/SW event trees is included in this table.

Likewise, it was found that sequences without seal LOCA were not significant contributors to core damage since the intervention of the AFW system (failure probability 3.4E-05) was considered enough to prevent the exceedance of the cladding temperature limit, even without CCW recovery. The global frequency of sequences without seal LOCA and with AFW failure is about 5.05E-8 which is below the cut-off level. The analysis then focused on seal LOCA sequences.

The lack of safety injection systems in the original event trees of Zion for loss of CCW/SW made them unusable for the SM2A study. It was necessary to generate new event trees. This was done with the support of simulation results, taking as a reference typical event trees for small and medium LOCA and without consideration of event time variability. The result is shown in Figure 8 which represents the seal LOCA sub-tree of a generic event tree for loss of CCW/SW.

Figure 8. Generic event tree for loss of CCW/SW with seal LOCA



For each seal leakage scenario, the most sensitive sequences to the power uprate were identified. It was found that the sequences with highest impact in PCT always involved failure of HPSI (probability 2.2E-05). A rough estimation of frequencies based on the Zion PSA data was performed. It was found that the collective frequency of these sequences (sequences 7 to 12 in Figure 8) was about 8.69E-09 which clearly falls below the cut-off frequency of 1E-07.

Sequence 6 is transition to Feed & Bleed and the frequency of this sequence is about 1.34E-08, also below the cut-off level.

Finally, sequences 3 and 4 involve failure of the RSIS header. This is reduction of the safety injection flow to avoid re-pressurization of the primary system. Although this header is present in the generic event tree, its activation depends on the particular values of the leak and injection flows. For the analyzed seal LOCA scenarios, this action has not been found demanded in any case. Therefore, sequences 3 and 4 are not present in our analysis.

The analysis was then oriented towards sequence 1 (red color in Figure 8). However, due to the introduction of time variability in headers RE and DEPRES, sequences 5 and 13 (green color in Figure 8) were also analyzed as a by-product of the analysis of sequence 1. Also, the time variability of these headers showed that this event tree does not describe all the existing possibilities. Delaying the CCW recovery and/or the SG depressurization may result in a new branching point in sequence 1 under the ACCS header with the consequence that some fraction of the sequence could result in limit exceedance.

Sequence 2 (black color) has not been analyzed in detail because it has been assumed that failure of the recirculation necessarily leads to limit exceedance. Therefore, sequence 2 contributes as a whole to the exceedance frequency with a value of 1.50E-07 y^{-1}.

In summary, the detailed analysis was performed on sequences 1, 5 and 13; sequence 2 was included in the quantification but not analyzed in detail and the estimated collective frequency of all the excluded sequences was about 7.26E-08, still below the cut-off level.

5.3. Simulation codes

The selection of the transient analysis code can be significantly conditioned by the specific approach used for exceedance frequency calculations. The application of the TSD theoretical framework naturally leads to the concept of damage domain and this was the approach of CSN for this exercise. The choice was advisable because it was expected that uncertainties were dominated by the occurrence times of stochastic events involved in the analyzed sequences.

At the time when SM2A was performed, this approach was still under development at CSN and, therefore, there was very little experience on its application. Under these circumstances, a high number of simulation runs was expected for a pilot exercise like SM2A.

The damage domain approach involves, at least from a conceptual point of view, two stages: damage domain searching and integration of the frequency density function. Being SM2A one of the pioneer applications of TSD, it was advisable to clearly separate these two stages. The number of required simulations for the first stage can be very high but it is in the second stage when the exceedance frequency is actually calculated. In order to speed-up the calculations, it was found recommendable to follow a graded approach consisting on using a fast, non-detailed code to find an approximate damage domain and then a detailed code to perform the final simulations.

For the purpose of damage domain searching, MAAP-4 (version 4.04) code was selected since it allows for modeling the essential parts of the plant while providing a reasonable speed and a relatively simple set of input data in terms of amount and complexity. In addition, the distribution of MAAP-4 includes a model for Zion NPP that required only minor modifications.

The second stage consists of simulating a sufficient number of transients belonging to the damage domain. A confirmation or a refinement of the damage domain is obtained as a by-product in this stage. These simulations provide the information needed to calculate probabilities and, at the end, the contribution of the sequence to the limit exceedance frequency. For this stage, it is desirable to use more powerful simulation models, given the potentially high influence of the occurrence times of relevant events, which should be calculated as accurately as possible.

The number of simulations needed for this stage can be optimized from the results of the previous stage. On the one hand, it is not necessary to simulate transients far from the tentative damage domain resulting from the first stage. On the other, an approximation to the frequency density function can be obtained from the results of the first stage, allowing for an optimization of the sampling density inside the damage domain, taking into account the expected variability of the frequency density function.

For the second stage, TRACE code was considered an ideal choice. However, the specific circumstances of the SM2A exercise made it impossible to setup the model for the analysis of the assigned sequences. The identification of the damage domains took longer than expected because there was no previous experience. Upon the end of the first stage the available time to setup the TRACE model and to perform all the required simulations was too short. It was then found more convenient to develop the second stage with the same MAAP model used for the damage domain identification. The disadvantage of a less accurate calculation was considered largely compensated by the possibility of checking the methodology in its whole extent. It should be noted that the purpose of SM2A was not to take a decision on a real power uprate but to show how the methodology can be applied for this purpose.

Although MAAP was already linked to the SCAIS system and the SM2A context was ideally suited for application of the SCAIS tools, most of the calculations were performed with MAAP standalone.

The linkage of MAAP to SCAIS, although already operative, could be considered in a debugging stage. Repeating the SM2A calculations with SCAIS-MAAP was indeed a good source of information for fine tuning of SCAIS.

5.4. Probabilistic calculations

The quantification of the original sequences of the Zion PSA did not require any specific tool. The available documentation at the time of the exercise contained very scarce information on the fault tree models used to quantify headers and sequences. In most cases, only the resulting conditional probability of each header was provided. Thus, the calculation of sequence frequencies is simply

$$\Phi_{seq} = \phi_{ini} \cdot \prod_{j} q_j \tag{5-1}$$

where ϕ_{ini} is the frequency of the initiating event and q_j are the conditional probabilities of the events in the sequence. In addition, only the nominal electric configuration was considered because any other configuration has much lower probability. For these simple operations, no PSA tool is needed.

For the purpose of exceedance frequency calculations, eq. (5-1) can also be applied to calculate the frequency of any particular transient Φ_{tr}. However, some complexities appear that should be discussed. The theoretical support is provided by the TSD (see ref. [14] and [19] for details). However, in the analysis of Loss of CCW sequences, all the stimulus activations and deactivations have been modeled as deterministic events, i.e., they occur when some specified dynamic conditions are reached. In this particular case the TSD equations get simplified to the expressions used below. Nevertheless, the formal derivation of these expressions from the general TSD has not been included in this document.

The first precaution in the application of eq. (5-1) is that the product extends only to stimulated events. A sequence or a transient containing a non-stimulated event is non-physical and must be discarded. This shows the importance of the concept of stimulus.

The occurrence of an event j may result in different outcomes i_j, each one with its own (conditional) probability P_{ji_j}, all of them summing-up to one. For example, when a multi-train system is started, each possible configuration of n/N trains is an outcome of the event (including the total failure 0/N) and the sum of their probabilities is 1.

Non-stochastic events are those that can only occur at the time of its stimulus (neglecting possible small and almost deterministic delays). It is the case, for example, of an automatic system which can only

start when its setpoint is reached. If the system does not start at this time, it does not start later (without further action) and we say that the system has failed. For this type of events, the value of q_j in eq. (5-1) is just the probability of the resulting outcome P_{ji_j}.

On the other hand, stochastic events occur after a random delay from the stimulus activation. The occurrence time is then characterized by a probability distribution. This is the case, for example, of operator actions that are delayed with respect to the point in time when they are demanded. The stimulus of the operator action can be an alarm condition or an instruction in an operating procedure. Events of this type have their probabilities distributed along some time period and the corresponding value of q_j in eq. (5-1) is the product of the outcome probability P_{ji_j} and a time probability ϑ_j.

Stochastic events are treated in PSA by assigning them an "available time". The event is considered "successful" if it occurs within the time window of the available time and "failed" if it occurs later or it does not occur at all. Success and failure probabilities are calculated accordingly. No difference is considered for different occurrence times within the available time. This type of modeling assimilates stochastic events to non-stochastic events in order to make them able to be processed by usual PSA tools since most of those tools, if not all, are unable to deal with time dependencies associated to stochastic events.

One of the advantages of the extensive use of simulation resources, as proposed by SMAP, is that it allows adequately taking into account time dependencies. In particular, probabilities of the stochastic events involved in the sequence can be calculated for each particular transient.

There are at least two ways to specify the variability in the occurrence time of a stochastic event. One is by specifying the occurrence rate, in general as a function of time with dynamic dependences $p(\vec{x},t)$. Given a particular dynamic history $\vec{x}(t)$, i.e., a plant transient, the occurrence rate can be described as a function of time only $p(t)$. The other is by specifying a time probability distribution, either by a probability density function (pdf) $h(t)$ or by a cumulative distribution function (cdf) $H(t)$. Pre-defined probability distributions can be used only when the delay of the event does not depend on the plant dynamics $\vec{x}(t)$. The relationships between these functions are the following:

$$H(t)=\int_0^t h(\tau)\,d\tau \quad ; \qquad 1-H(t)=\exp\left(-\int_0^t (\tau)\,d\tau\right);$$

$$h(t)=p(t)\left(1-H(t)\right) \tag{5-2}$$

In these expressions the origin of time is always the activation of the stimulus.

In some cases, an active stimulus becomes deactivated before its associated event occurs. Deactivation of the stimulus could result from the evolution of the dynamic conditions or from the occurrence of other events. Should this happen, the occurrence rate of the associated event becomes zero and the event cannot be expected to occur anymore (unless the stimulus is reactivated later). Non-occurred, stimulated events are also important for quantification of exceedance frequencies.

For stochastic events, the value of the time probability ϑ_j depends on the activation, deactivation and occurrence times. Two cases should be considered:

1. The stimulus was activated at t_s but the event did not occur at any time along the transient. It could happen that the stimulus became deactivated at a time t_d or that the end of the transient came (most often because the damage condition was reached) before the occurrence of the event, without previous stimulus deactivation. In the latter case we say that $t_d = t_{end}$. For this type of non-occurred events, the value of ϑ_j that should be used is the so-called survival probability, given by $1 - H_j\left(t_d - t_s\right)$.

2. The stimulus was activated at t_s and the event occurred at t_e or, more exactly, it occurred between t_e and $t_e + dt$. In this case, the time probability is given by $\vartheta_j = h_j\left(t_e - t_s\right)dt$. Note that h_j is not a probability but a probability density and we need dt to maintain the correct units.

Let us now consider a particular dynamic sequence, i.e., the set of all the possible transients sharing the same set of **occurred** events. Let us assume for now that the only uncertainty in this sequence is associated to uncertain times of stochastic events. Transients in this dynamic sequence could differ in the occurrence time of stochastic events or in the stimulated, non-occurred events they contain. For any particular transient in this sequence, eq. (5-1) can be rewritten as:

$$\Phi_{tr} = \phi_{ini} \cdot \prod_j P_{ji_j} \cdot \prod_k \left(1 - H_k\left(\Delta t_k\right)\right) \cdot \prod_l P_{li_l} h_l\left(t_l - t_{sl}\right) dt_l \tag{5-3}$$

where index j indicates non-stochastic events, index k is for stochastic, non-occurred events and index l stands for stochastic, occurred events. Note that each occurred stochastic event introduces a differential factor and Φ_{tr} becomes differential in as many dimensions as occurred stochastic events:

$$\Phi_{tr} = Q\left(t_1, \cdots t_{l_{max}}\right) \prod_l dt_l \tag{5-4}$$

A geometric interpretation of the space defined by all the t_l allows defining the concept of sequence volume as the set of all the physically possible combinations of occurrence times of the stochastic events in the sequence. The sequence frequency would result from the aggregation of (5-4) for all the transients in the sequence. Using the concept of sequence volume, the aggregation can be expressed as:

$$\Phi_{seq} = \int_{V_{seq}} Q\left(t_1, t_2, \cdots t_{l_{max}}\right) dt_1 \cdot dt_2 \cdots dt_{l_{max}} \tag{5-5}$$

Eq. (5-5) shows that stochastic, occurred events have the effect of distributing the sequence frequency across the sequence volume. The integrand of (5-5), $Q\left(t_1, t_2, \cdots t_{l_{max}}\right)$, is the frequency density at each point of the sequence volume, i.e., the frequency density that corresponds to each transient belonging to the sequence. Among these transients, some could lead to generation of unacceptable damage (defined in terms of exceeding a required limit) while others would finish in a stable safe state. The former define a subset of the sequence volume which is called the *damage domain* of the sequence.

The contribution of the sequence to the exceedance frequency of a given limit would be given by an expression similar to (5-5) but extending the integral only to the damage domain of the sequence:

$$\Phi_{seq}^{ex} = \int_{D_{seq}} Q\left(t_1, t_2, \cdots t_{l_{max}}\right) dt_1 \cdot dt_2 \cdots dt_{l_{max}} \tag{5-6}$$

5.5. Modification of the sequence models

In the previous section it has been shown how the application of the TSD requires the use of dynamic sequences instead of PSA sequences. Transients grouped in a PSA sequence are assumed to contain the same set of both occurred and failed events. Instead, transients in a dynamic sequence contain the same occurred events but may differ in the non-occurred (i.e., failed or non-stimulated) events. In addition, the concept of stimulus, which is essential for the application of TSD, is not explicit in the classical PSA approach. Also, it has been found that the use of dynamic sequences provides a better coverage of the risk space.

As a consequence of the above, the calculation of the exceedance frequency resulting from loss of CCW/SW cannot be performed on the PSA event tree of Figure 8. It was already indicated in section 5.2 that this event tree does not describe every possible occurrence. Nevertheless, the initial screening performed at PSA sequence level was not useless since it provided valuable information to configure the analyzed dynamic sequences.

The nomenclature for dynamic sequences that was used in this analysis is as follows: each event is represented by a letter, uppercase letters representing events actually occurring and lowercase letters representing non occurring events. The dynamic events that have been considered are the following:

I Initiating event: loss of CCW or SW systems.

K Reactor trip. Manually initiated by operators and including shutdown of reactor coolant pumps.

F Initiation of the AFW system.

B seal LOCA, equivalent to a small or medium break.

H HPSI initiation. Automatically initiated upon the coincidence of two conditions: pressure below an initiation setpoint and recovery of CCW. One pump in operation assumed (success criterion of the Zion PSA).

A Accumulator injection. Automatically initiated at a given RCS pressure. Three out of four accumulators are assumed to inject water, as in the reference PSA.

L LPSI initiation. Automatically initiated with the same conditions (including same setpoint) of HPSI. Note that initiation of LPSI (or HPSI) means that the system is started-up, but the water flow actually injected depends on the primary system pressure and can be even null. The success criterion of the Zion PSA (1 out of 2 pumps) has been assumed again.

S Cooling through steam generator relief valves. Manually initiated by operators when requested by operating procedures. A cool-down rate of 55 ºC/h has been assumed.

R Recovery of CCW. Manual action requested from the occurrence of the initiating event.

It has been mentioned that our analysis included only sequences with seal LOCA. Among them, sequences with failure of **K**, **F**, **H** or **L** were excluded because of their low frequency. Occurrence times of **B**, **S** and **R** were considered uncertain. Although **K** is also a manual action, its occurrence time is much less uncertain and, for the sake of simplicity, it was considered coincident with the initiating event.

With these considerations, the main focus of the analysis was on the dynamic sequences **KFBRHSAL** and **KFBRHSaL** and their possible permutations in the order of the events. These sequences were expected to be the main potential contributors to the exceedance frequency. Note that the second of these sequences includes not only transients with failure of accumulators but also transients where the accumulators are not demanded.

However, long delays in the occurrence of **R** could result in the exceedance of the PCT limit before the recovery. Since **R** conditions both **H** and **L**, these situations are represented by dynamic sequences **KFBrhSaI** or **KFBrhSAl**, both of them potential contributors to the exceedance frequency since they only involve the failure (excessive delay) of **R** over the originally selected sequences. Note that the lack of actuation of both **H** and **L** is not due to their own failure but a direct consequence of the lack of recovery. Something similar occurs if **S** is delayed and the resulting sequence is **KFBRHsaL**, where the lack of accumulator injection is due to the maintenance of high pressure. Finally, if both manual actions are excessively delayed, the resulting sequence is **KFBrhsal**. This sequence does not contribute very much to the exceedance frequency but was included in the analysis for the sake of completeness.

5.6. Modification of some header models

Seal LOCA model:

A model for seal LOCA was needed. On the one hand, the occurrence time assumed in the Zion PSA was not uncertain and the occurrence probabilities were concentrated at specified times. On the other, the probability of the seal LOCA was found overestimated. After some documental review (ref.[20], [21], [22], [23]), it was proposed and accepted by the SM2A Task Group to use a model very similar to the one developed by the Westinghouse Owners Group, named WOG 2000. The proposed model contains a number of strong simplifying assumptions but a more realistic model would introduce excessive and unnecessary complexity.

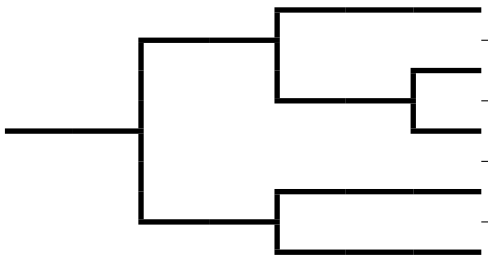
In this model, the total (i.e., for time $\rightarrow \infty$) failure probabilities for each sealing stage are the following:

- 1st stage: 0.0125
- 2nd stage: 0.2
- 3rd stage: 0.27

Failures of sealing stages are assumed lognormally distributed in time. The time distribution is determined by setting its 5th percentile at 15 minutes and its 95th percentile at 60 minutes after the total loss of seal cooling. The resulting parameters of the lognormal distribution (with time in seconds) are: $\mu = 7.4955$; $\sigma = 0.4214$. The stimulus of the seal LOCA is the loss of seal cooling (LOSC), which is assumed to occur at $t = 0$.

The possible leakage scenarios with their associated leakage per pump and conditional probabilities are defined in the decision tree of Figure 9.

Figure 9. Seal LOCA leakage scenarios



LOSC	Seal 1	Seal 2	Seal 3	Scenario	Leakage Per pump (gpm)	Leakage Per pump (m^3/s)	Condit. Probab
				1	21	1.32E-03	0.79
				2	57	3.60E-03	0.144
				3	182	1.148E-02	0.053
				4	76	4.79E-03	0.01
				5	480	3.028E-02	0.0025

Each one of the specified leakage scenarios should be evaluated and weighted with its own probability. The analysis of the loss of CCW/SW started with scenario number 3 and it became soon evident that the SM2A mandate was too short to include more scenarios. It was decided to restrict the analysis to this scenario but assigning to it the total probability of seal failure, i.e., the sum of probabilities of scenarios 2 to 5 (note that scenario 1 is the no failure case) which results 0.21. This probability value acts as a multiplier of the time probability distribution above defined.

CCW/SW recovery model:

A probability of 0.13 has been used in the Zion PSA for the failure of CCW/SW recovery. This value refers to the probability of non recovery with enough time as to avoid core damage. However, there is no indication of the available time value that has been used to calculate this probability.

Looking at the analysis results of the dynamic sequence **KFBRHSaL**, which is our main contributor to exceedance frequency, it can be seen that there is no damage if the recovery occurs before 10,000 seconds. We can then take this value as the available time. Assuming a lognormal distribution for the recovery time and determining two points of this distribution, the recovery time can be fully characterized. One of the points is given by the 0.13 probability of recovery before 10,000 seconds. The second point is derived from the consideration that the recovery is very unlikely during the first 15 minutes. A 5% was assumed for this probability.

With these considerations, the recovery time (in seconds) would be characterized by a lognormal distribution with parameters $\mu = 8.2319$; $\sigma = 0.8690$. No multiplier should be applied to this distribution. The stimulus of the CCW/SW recovery is the loss of the system which is assumed to occur at $t = 0$.

Secondary side depressurization and cooling:

The available information about the Zion PSA did not provide probability values for this event. Depressurization through steam generators is embedded with Auxiliary Feedwater in a single header and there is no separate information about each event.

It has been assumed that the time distribution follows a lognormal law and a Westinghouse three-loop plant has been used as a reference for probability estimation. The probability value used in the PSA of that plant was not directly applicable because it had been calculated assuming an available time (about 10,000 seconds) which was found inconsistent with Zion simulation results. The required execution time was 1800 seconds. Changing the available time to 7500 seconds and maintaining 1800 seconds as required time resulted in an approximate probability value of 0.95 to complete the action within 7500 seconds. A probability of 0.05 to complete the action in less than 1800 seconds was also assumed.

The parameters of the resulting lognormal distribution, with time in seconds, are: $\mu = 8.2091$ and $\sigma = 0.4338$. The stimulus for the secondary side depressurization, i.e., the time origin for the distribution, is the occurrence of the seal LOCA.

Probabilities of non-stochastic events:

For non-stochastic events, the conditional failure probabilities were taken from the Zion PSA. The only failures allowed in our study were the accumulator system and the recirculation. The accumulator system is not modeled as a separate header in any scenario of the Zion PSA. It is included in the Low Pressure Injection header for Large Break LOCA but excluded from the analogous header for Medium Break LOCA. The comparison of the probabilities of both headers allowed estimating the accumulator-only failure probability. The failure probability values used for Safety Injection Systems are:

- High pressure injection: $p_{HPIS} = 2.2E\text{-}05$
- Low pressure injection: $p_{LPIS} = 5.6E\text{-}04$
- Accumulator system: $p_{ACC} = 9.4E\text{-}04$

However, both p_{HPIS} and p_{LPIS} are irrelevant for this analysis since sequences with failures of these systems have been screened-out (see 5.2).

5.7. Base case simulations

A set of initial simulations was performed in order to setup adequate steady state initial conditions both for initial and uprated power and for supporting the initial sequence screening.

The steady states used as initial conditions for transient simulations are summarized in Table 2.

Table 2. Steady state simulation results

Variable	Units	100%	110%
Primary side			
Power	[MWth]	3236	3560
Pressurizer pressure	[MPa]	15.6	15.6
Cold leg temperature	[K]	559.9	558.2
Hot leg temperature	[K]	594.2	595.9
Core flow rate	[kg/s]	4259	4259
Axial power distribution		Max APF=1.28	Max APF=1.28
Radial power distribution (power levels for different fuel pins represented in the model)	[kW/m]	32.9	36.2
Secondary side			
Steam Generator pressure	[MPa]	5.07	5.07
Steam Generator level	[m]	7.5	7.5
Steam Generator inventory	[t]	40.7	40.7
Secondary side feedwater flow rate	[kg/s]	1760	1934
Secondary side feedwater temperature	[K]	493.3	493.3

The results of the transient simulations performed at 100% initial power for supporting the initial sequence screening are presented in tree format in Figure 10 (ref. [16]). No time variability was introduced in these simulations. It was assumed that CCW system recovery occurs at the time of the seal LOCA, so that Safety Injection systems are available, if they do not fail. The depressurization of the steam generator secondary side, if not failed, is assumed to occur 600 seconds after the LOCA.

Figure 11 shows the evolution of primary system pressure and cladding temperature for the transients of Figure 10 (ref. [16]). Table 3 summarizes the safety variable (cladding temperature) results for each sequence.

All the base case sequences resulting in limit exceedance involved failures of more than one system and, therefore, their frequencies are well below the cut-off value. The analysis was then oriented towards the nominal sequence. Note that the introduction of time variability in the nominal sequence opens the possibility of reaching damage conditions due to excessive delay in protective actions. Also, for some delay values, the primary pressure can fall below the accumulator injection pressure and the possibility of accumulator failure should be taken into account. The selection of sequences for uncertainty analysis was discussed in 5.2.

Figure 10. Base case sequences for loss of CCW/SW analysis

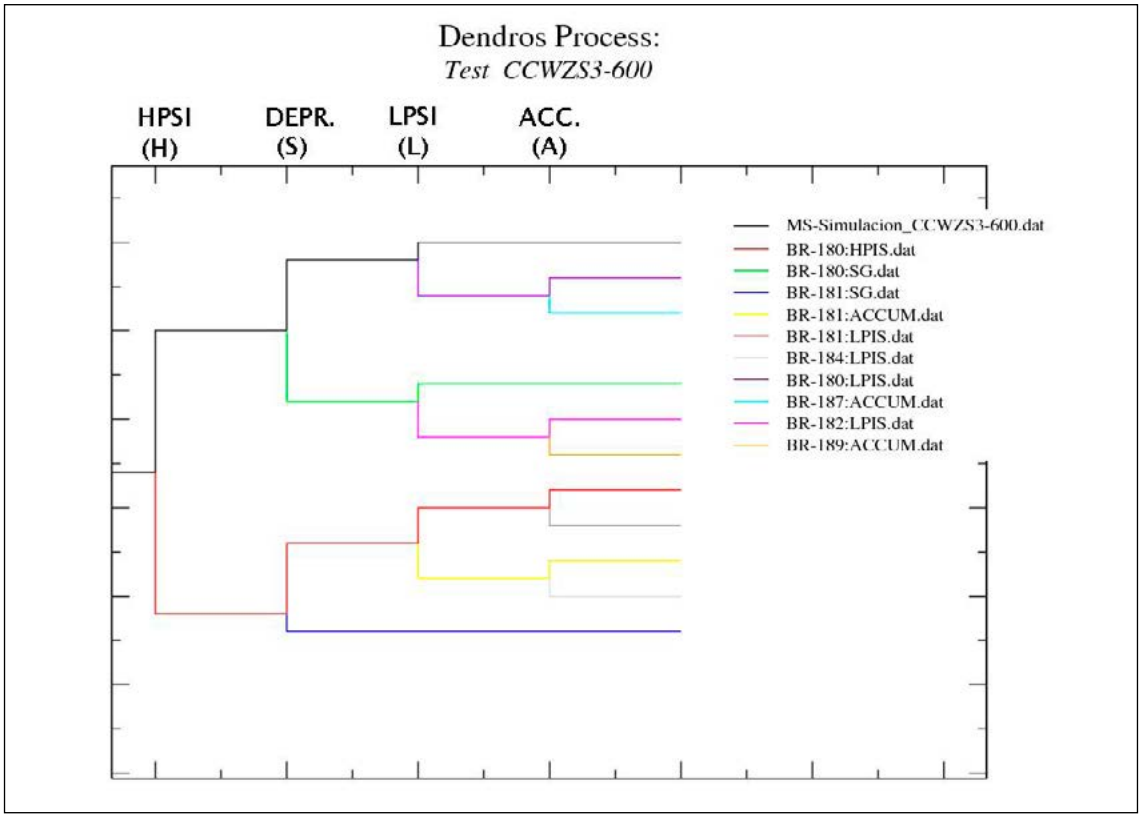


Figure 11. Loss of CCW/SW base cases. Primary system pressure and core temperature

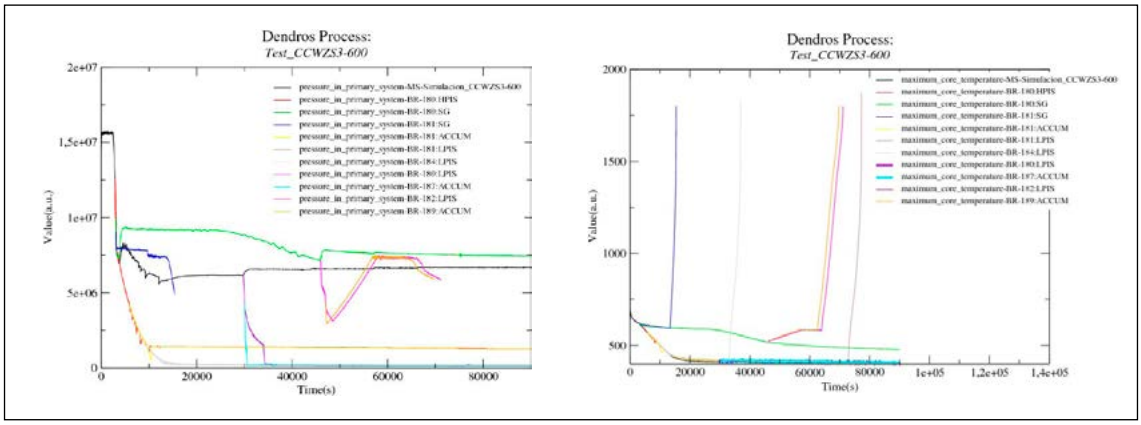


Table 3. Safety variable values for base case simulations

Sequence	Limit comdition time	Time for max. temperature	Peak clad temperature
HSL	—	100 sec.	690 K
HS$\overline{\text{L}}$A	—	4,000 sec.	405 K
HS$\overline{\text{LA}}$	—	4,000 sec.	405 K
H$\overline{\text{S}}$L	—	3,100 sec.	620 K
HS$\overline{\text{L}}\overline{\text{A}}$	71,146 sec.	71,146 sec.	DAMAGED
HS$\overline{\text{LA}}$	69,764 sec.	69,764 sec.	DAMAGED
$\overline{\text{H}}$SLA	—	2,935 sec.	621 K
$\overline{\text{H}}$S$\overline{\text{L}}$A	77,276 sec.	77,276 sec.	DAMAGED
$\overline{\text{H}}$SL$\overline{\text{A}}$	—	5,869 sec.	570 K
$\overline{\text{H}}$S$\overline{\text{LA}}$	36,900 sec.	36,900 sec.	DAMAGED
$\overline{\text{HS}}$	16,515 sec.	16,515 sec.	DAMAGED

5.8. Uncertainty analysis

Loss of CCW/SW scenarios involve actions and events occurring at very uncertain times. The time variability in events such as the occurrence of the seal LOCA, the recovery of the CCW system or

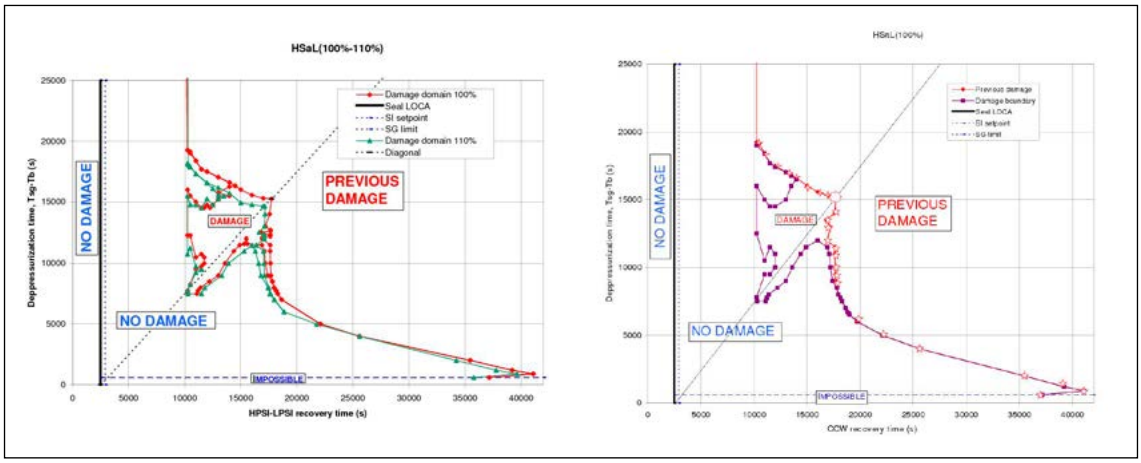
the depressurization and cooling through the secondary system has a very important effect on the evolution of the plant state after the accident. Even ignoring the time variability of other actions such as the reactor trip or reactor coolant pump shutdown, it was estimated that time uncertainties would have a dominant effect with respect to model parameter uncertainties. In addition, it was considered that the analysis of parametric uncertainties with a non-detailed thermalhydraulic model (see 5.3) would add low value to the study. Consequently it was considered convenient to focus on time uncertainties only.

The first step in the damage domain approach for uncertainty analysis is the determination of damage domains (ref. [16]). As above discussed, the main focus of the analysis has been on dynamic sequences with no system failure. The nominal sequence in Figure 10 shows intervention of High Pressure and Low pressure Injection systems, but no accumulator demand. It should be recalled that success of Low Pressure Injection means only that the pumps have been successfully started, but not necessarily that they have been able to inject water into the system. The lack of accumulator injection demand indicates that the pressure has remained above the point where low pressure injection is possible. In terms of the dynamic sequence nomenclature of section 5.5, this type of scenarios is identified as **KFBRHSaL**. However, as longer values of uncertain times are considered, it is found that, in some cases, there is accumulator demand. In other words, this dynamic sequence includes some cases involving accumulator failure, which must be adequately accounted for in the frequency calculation.

Since there are three uncertain times involved in this sequence, namely, occurrence of LOCA, recovery of CCW and depressurization of the secondary side, the damage domain is three-dimensional. This makes it difficult to graphically represent the damage domain in an illustrative way. For the only purpose of graphical representation, it was decided to consider a fixed value of the occurrence time of seal LOCA and to represent two-dimensional damage domains using recovery time and depressurization time as coordinate axes. As an additional approximation, it was considered that the shape of the represented two-dimensional damage domain is independent of the third dimension (time of the seal LOCA). This approximation is equivalent to consider constant decay heat which is not very realistic but allows for a drastic reduction in the number of simulations for the second stage of the analysis (integration of the frequency density).

Figure 12.a shows the bi-dimensional damage domain of the dynamic sequence **KFBRHSaL** for 100% initial power and seal LOCA occurring 2500 seconds after the reactor trip. There are three main regions in this figure, labeled as “NO DAMAGE”, “DAMAGE” and “PREVIOUS DAMAGE”, respectively. There is also a small area of “IMPOSSIBLE”, i.e., non-physical transients. The closed “DAMAGE” area is the bi-dimensional damage domain of **KFBRHSaL**. However, this is not the only represented damage domain. The red line boundary between “PREVIOUS DAMAGE” and the other regions represents the damage domain of other dynamic sequences. This boundary is divided in two parts by the dashed straight line representing the points where depressurization and recovery are simultaneous.

Figure 12. Damage domains of the dynamic sequence KFBRHSaL and its associates



a) Damage domains at 100% b) Comparison between 100% and 110%

The upper part of the boundary, marked with four-point stars, represents points where depressurization is so delayed that the damage comes first. Once the damage has occurred, the actual time of the depressurization is irrelevant and the effect is the same as the depressurization failure. As discussed in Section 5.5, these points belong to a different dynamic sequence, namely, **KFBRHsaL**, and represent the damage domain of this sequence. Note that, since one of the uncertain times has been eliminated, the damage domain is no longer a surface but a line. The ordinate of the points in this line should not be interpreted as depressurization time but as damage time.

Analogously, the lower section of the boundary, marked with five-point stars, represents points where damage comes before recovery, i.e., points belonging to the dynamic sequence **KFBrhSaL**, as discussed in Section 5.5. This section of the boundary is, therefore, the damage domain of that sequence and the abscissa of these points is now the damage time.

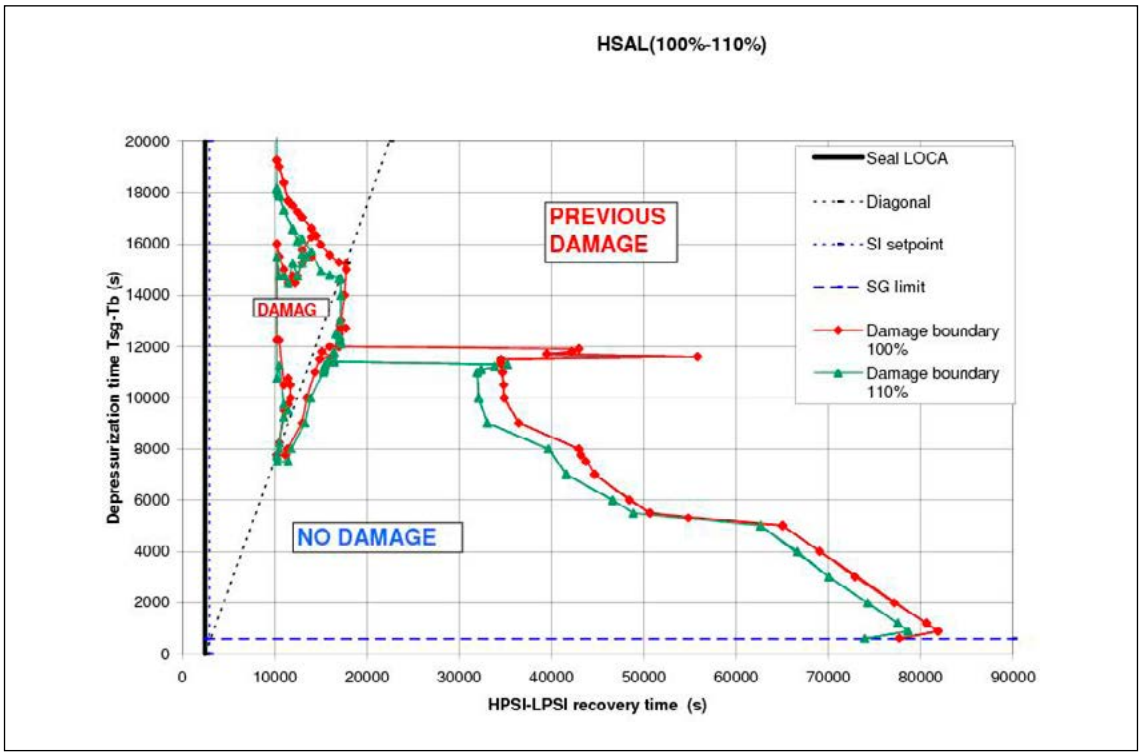
Finally, the point marked with an eight-point star, is the point where both depressurization and recovery events are delayed beyond the damage time. It is, then, the only point of the sequence **KFBrhsal**.

Since sequences **KFBRHsaL**, **KFBrhSaL** and **KFBrhsal** result from the elimination of stochastic events from **KFBRHSaL**, we consider them associated to the latter. Figure 12.b shows the comparison of damage domains of all these sequences for 100% and 110% initial power. It should be recalled that, when the variability of the occurrence time of the LOCA is considered, all these damage domains increment their dimension by one.

Most of the points in these damage domains correspond to transients where there is no accumulator demand. However, there are also some points where no actuation of accumulators is due to a system failure. Taking into account that sequences without system failures have a higher frequency, it was considered convenient to include in the exceedance frequency quantification the dynamic sequence **KFBRHSAL** and its associates.

The effect of not forcing accumulators to fail if demanded is shown in Figure 13. This figure represents the damage domain of the dynamic sequence **KFBRHSAL** (and associates) along with the fraction of **KFBRHSaL** where accumulators are not demanded. Note also that the only dynamic sequence associated to **KFBRHSAL** is **KFBrhSAl**, since the failure of **S** prevents accumulator demand.

Figure 13. Damage domain of sequences without system failure



All these sequences have been included in the exceedance frequency quantification. The results are discussed in Section 5.9 below (ref. [16]).

Once the damage domains for the specified sequences were identified, a uniform grid was used to evaluate and integrate the frequency density function inside the damage domains. The sampling time

interval for both depressurization and seal LOCA was 500 seconds. The recovery time was sampled every 1,000 seconds. Note that only the mesh points inside the damage domains need to be evaluated. For the seal LOCA the occurrence time was allowed to vary between 1,000 and 4,000 seconds.

The total number of transients that contributed to the exceedance frequency quantification was 1,022 for each value of the initial power, although only 146 of them were actually simulated. The simulated transients correspond to the nominal LOCA time of 2,500 seconds. The remaining ones were estimated with the assumption of constant residual heat and were obtained by shifting the calculated transient in the amount of the difference between the assumed LOCA time and 2500 seconds.

5.9. Evaluation of exceedance frequency (results)

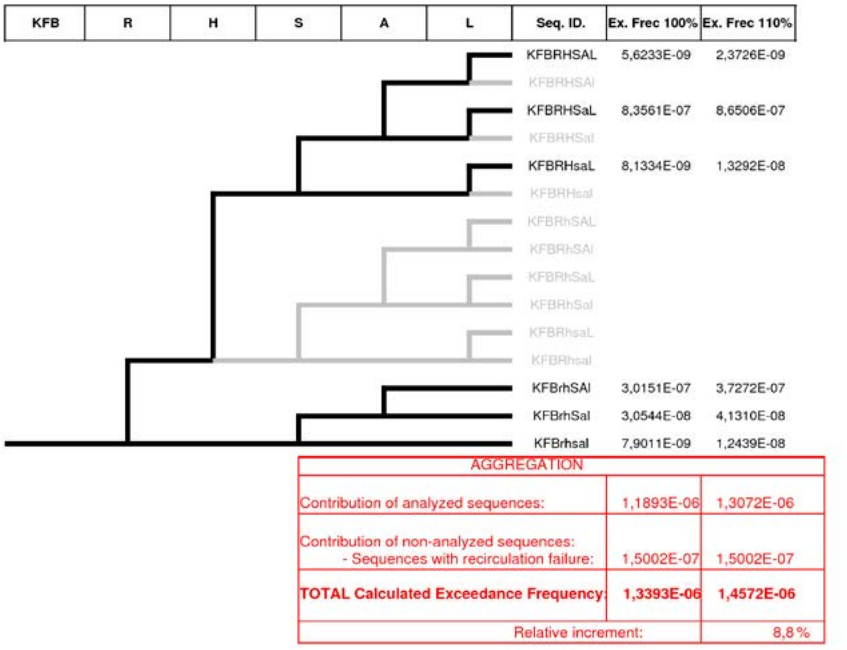
The results of the exceedance frequency quantification for sequences without recirculation failure are summarized in the dynamic tree of Figure 14 (ref. [16]). Note that the interpretation of this event tree differs from a PSA event tree in the following points:

- Branching points do not represent success or failure states. They rather represent occurrence or not without judgment about the need or the convenience of the event. This aspect is evaluated only at individual transient level.

- The frequency values displayed on each dynamic sequence are not the whole sequence frequency but only the contribution of the sequence to the total exceedance frequency of the limit.

- Any possible transient in the plant that matches the initial branch (KFB in this case) can be classified in one and only one sequence of the tree. Non represented sequences are considered non-physical.

Figure 14. Dynamic event tree for exceedance frequency quantification



Bold lines in this event tree correspond to the sequences that resulted from the discussion in Section 5.8 above, i.e., the sequences that have been actually quantified. Shadow sequences have not been quantified but are expected to result in negligible contributions.

It is observed that the main contributors are sequences **KFBRHSaL** and **KFBrhSAl**. Both of them are sequences with, at most, one failure. Most of the **KFBRHSaL** sequence contribution comes from transients without accumulator demand (therefore, without accumulator failure) and the cause of the damage is excessive delay in the operator actions. Sequence **KFBrhSAl** contains only the failure of operator action **R**.

The nominal sequence **KFBRHSAL** gives the lowest contribution. Although this is the most probable sequence, this result could be expected because in this sequence all the systems perform as expected. The only contribution to damage comes again from excessive delays in operator actions which are also very unlikely.

The remaining sequences, which were obtained almost as a by-product of the main contributors, give negligible results and could be ignored. They have been retained, however, because they are considered very illustrative for the application process of the methodology.

The table in the lower part of Figure 14 shows the final results. The "Contribution of analyzed sequences" is the summation of the contributions of all the quantified sequences in the dynamic tree for each initial power level. As above indicated sequences with recirculation failure contribute as a whole and have not been analyzed. Their contribution is not sensitive to the initial power level and the indicated value has been taken from Section 5.2 above. The "TOTAL calculated exceedance frequency" is given for each power level. These results show that the contribution to the exceedance frequency of loss of CCW/SW scenarios increases an 8.8% due to the power uprate.

Appendix A. Comparison exercise on uncertainty analysis methods

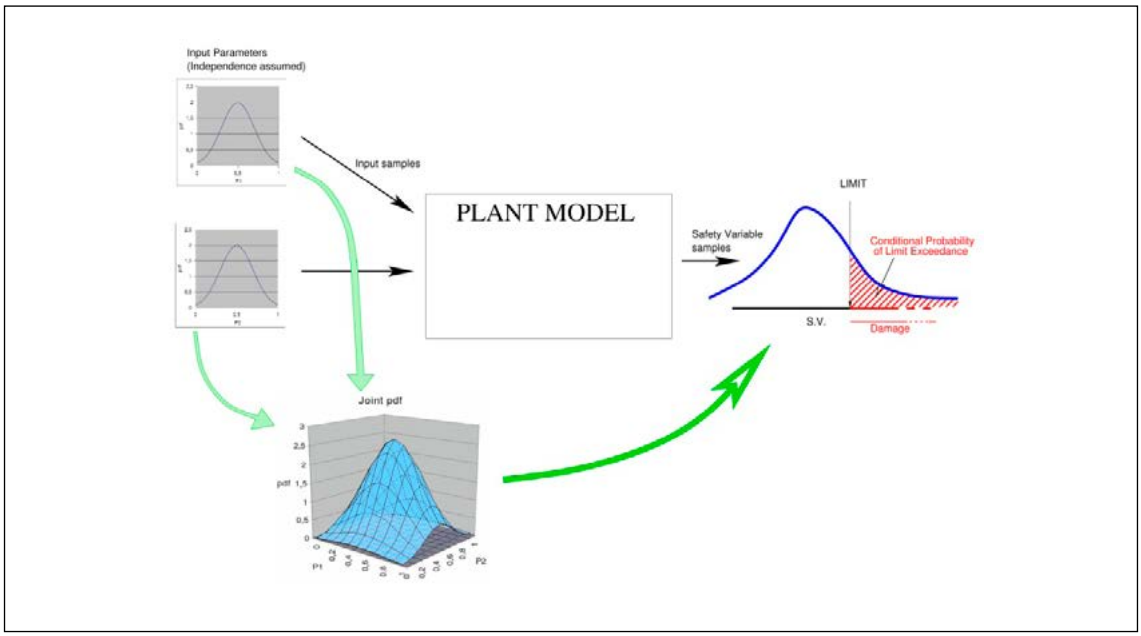
Appendix A. Comparison exercise on uncertainty analysis methods

From the discussions and examples given throughout this document it becomes quite clear that the assessment of safety margins is but a particular case of uncertainty analysis, supported by sequence simulation.

Most of the usual approaches to uncertainty analysis of plant simulations are based on the use of random sampling techniques with different variants like simple, biased or stratified sampling. The main idea behind these techniques is to propagate the uncertainty distributions of model inputs, model parameters and others to the simulation output in such a way that an uncertainty distribution can be associated to the safety variable of interest.

Depending on the particular purpose of the uncertainty analysis, the needed level of knowledge on the output distribution is different but in any case the objective is to calculate, to estimate or to bound the integral of the output distribution over the region of unacceptable values of the output variable. As discussed in 2.2, the acceptability of the safety variable values can also be defined in terms of a probability distribution. In this case, a convolution should be performed instead of a simple integration (see eq. 2-2). In the following discussion, however, it is assumed that a discrete safety limit is the boundary between acceptable and unacceptable values of the safety variable (safety limit approximation in terms of 2.2)

Figure 15. Propagation of input uncertainties to simulation output

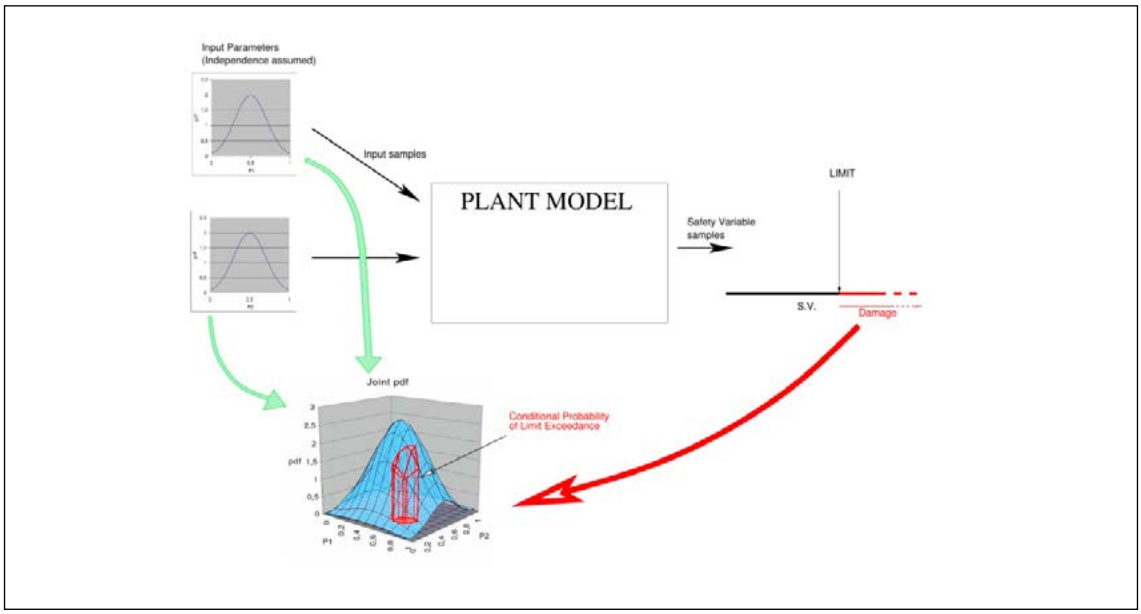


The uncertainty propagation approach is schematically described in Figure 15 for uncertain input parameters only. By sampling input parameters using their probability distributions and using adequate statistical methods, the joint input probability distribution (blue surface in figure 15) is propagated through the simulation model and a distribution of the safety variable can be estimated. The red area under the output distribution represents the conditional probability of limit exceedance.

On the other hand, it has been shown how the application of the TSD framework leads to the concept of damage domain and to the integration of the frequency density function over the damage domain. From the point of view of uncertainty analysis, this approach is equivalent to replace the forward propagation of the uncertainty distributions by the backward propagation of the range of unacceptable output variable values. This process allows identifying, based on simulation results, the range of combinations of uncertain elements that end in an unacceptable output value, i.e., the damage domain. Then, the conditional exceedance probability is calculated by integrating the joint probability density of the problem uncertainties over the identified damage domain.

For the simple case of input uncertainties only, the damage domain approach is schematically described in Figure 16. In this figure, the damage domain is the base of the red cylinder drawn on the joint input space and the conditional exceedance probability is the volume of this cylinder under the joint probability density function.

Figure 16. Back-propagation of the damage domain to input uncertainty distribution



The same approaches can be applied also for more complex combinations of uncertainties (ref. [24] and [25]). It is a matter of efficiency and availability of resources to select the most convenient approach.

When the uncertainties in a given problem depend on the dynamics of the physical system and especially when there are uncertain times associated to stochastic events, the calculation of the joint probability distribution or the generation of random input samples become more difficult tasks. The TSD framework has been developed to adequately address these cases. It provides means to calculate the joint probability density function taking into account the results of multiple simulations (dynamic dependences) and is especially suited for the application of the damage domain approach.

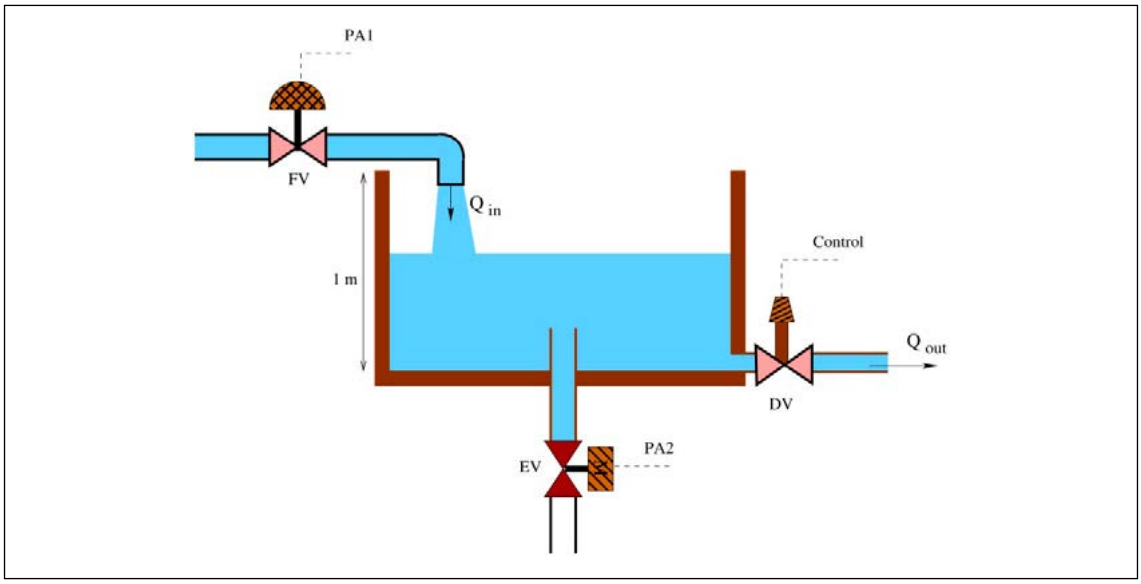
The exercise here described has been developed, on the one hand, to check the equivalence of the two basic approaches and, on the other to try to discover some criteria for selecting one approach or the other. The two approaches have been found equivalent in all the analyzed cases. However, the exercise cannot be considered in any way as a formal demonstration of the equivalence and its only purpose is to better understand the methodologies with their advantages or disadvantages.

To this aim, a very simple physical system has been selected to analyze different configurations and combination of uncertainties. Using a very simple system with very basic safety features has two main advantages. First, the system physics is so simple that the meaning of the simulation results is straightforward and all the analysis power can be concentrated on the uncertainty aspects. Second, a huge number of simulations can be done in a short time in order to get enough accuracy as to make the results of the two approaches comparable.

A.1 System description

More than 90% of the times that somebody thinks of a very simple physical system, he or she has a tank in mind. To this respect, the exercise has not been very original: the physical system is a tank which is represented in Figure 17.

Figure 17. Schematic of the tank system



Water is supplied to the tank with volume flow rate Q_{in}. In normal operation Q_{in} remains constant. There is also a normal drain line taking water out of the tank at Q_{out}. A control system is assumed to maintain constant the tank level, i.e., $Q_{out} = Q_{in}$ in normal operation. The control system has been assumed perfect and instantaneous and has not been modeled.

There is also a protection system that tries to avoid tank overflow in case that the drain pipe gets partially or totally clogged. The safety variable is, therefore, the water level and the safety objective is to maintain this level below the safety limit defined by the tank height (1 m). To this aim, two protective actions (PA) are provided:

- **PA1**: closure of the pneumatic feed valve. This makes the feedwater flow decrease at a constant rate until the valve gets closed. However, due to long term variations in the air pressure, the closing time of the valve T_{in}^{cl} (which will be shortened to t_c) has an uncertain value, uniformly distributed between 20 and 36 seconds.

- **PA2**: opening of the motor-driven emergency drain valve. When opening, the flow through this valve increases at a constant rate until the drain flow reaches its maximum value Q_{ev}^{max}. The opening time of this valve is $T_{ev}^{op} = 60$ seconds

Protection interventions are driven by two alarm signals:

- High level: 0.95 m.
- High-high level: 0.98 m.

In some of the analyzed cases the protections will be automatic while in others they will be initiated by operators.

The only accident to be considered is the clogging of the normal drain pipe. The drain pipe is designed to drag small objects, so the minimum possible blockage is equivalent to 50 % of the drain flow. This accident is described by the following parameters:

- Estimated frequency of clogging incidents of any size: $\nu_{ini} = 2\,y^{-1}$.
- The clogging fraction, represented by s , of the drain flow varies from 0.5 to 1 with a probability density given by $f(s) = -7.2s + 7.4$.

The clogging fraction is treated as a multiplier of the initial drain flow. No effect from the control system is assumed during the transient. The overflow frequency will be given by the product of the initiating event frequency ν_{ini} . and the conditional probability of limit exceedance P_{ex} . The analysis is focused on the calculation of P_{ex} since ν_{ini} is a constant value.

Although the comparison was performed for four different cases, only two of them are reported here. In the first case the protection is fully automatic and in the second one both protective actions are manual and the probabilities of their delays depend on the dynamic conditions. These two cases are the simplest and the most complex ones of those analyzed during the exercise.

A.2 1st. analysis case: automatic protection

The high-level signal is the setpoint to initiate the closure of the feed valve while the high-high-level signal initiates the opening of the emergency drain valve. In this case, there are only two uncertain parameters involved. One is the fraction of flow being blocked at the drain pipe and the other the closure rate of the feed valve.

The objective of the analysis is to calculate the conditional probability of tank overflow. The calculation has been done by two methods:

- Propagation of the parametric uncertainties.
- Identification of the damage domain and integration of the frequency density.

Propagation of input uncertainties

Random sampling has been applied to obtain samples of the uncertain parameters. Random samples of an uncertain parameter are obtained from the inverse of its cumulative distribution function. For the clogging fraction of the drain pipe the sampling function is:

$$s = \frac{3.7 - \sqrt{13.69 - 3.6\left(2.8 + R\right)}}{3.6} \tag{A-1}$$

where R is a random number[1] between 0 and 1.

For the closing time of the feed valve, the sampling function is:

$$t_c = \frac{R + 1.25}{0.0625} \tag{A-2}$$

with R being also a random number between 0 and 1.

The estimation of the conditional probability of limit exceedance, based on the calculation of random samples and represented by $\tilde{x}$, is a random variable. The variance of the estimated value is a function of the probability value being estimated and the number of samples:

$$Var\left(\tilde{x}\right) = \frac{x\left(1 - x\right)}{N} \tag{A-3}$$

where x is the "true" probability value being estimated and N is the number of samples. The estimated value of x is given by $\tilde{x} = n / N$, where n is the number of the calculated samples that resulted in limit exceedance. The accuracy of the estimation, represented by an error band (the narrower error band, the higher accuracy), is related to its standard deviation σ. Assuming a normal distribution for the probability estimation, an interval of $\pm 3\sigma$ will include the 99.7% of the estimates. Therefore, if the desired accuracy of $\tilde{x}$, with a confidence level of 99.7%, is $\pm A_x$, the minimum number of samples that will be needed is,

$$N = \frac{9x\left(1 - x\right)}{A_x^2} \tag{A-4}$$

[1] Random numbers in the sampling functions will be represented by R. However, each R is independently generated.

In the application of equations (A-3) and (A-4) it is acceptable to use $\tilde{x}$ instead of x except for low values of N. An initial estimation of the conditional overflow probability for this analysis case resulted in a value around 0.06. The application of (A-3) for different values of N resulted in the following relationship between number of samples and resulting accuracy:

Table 4. Expected accuracy of the overflow probability (case 1)

No. of samples	Variance	σ	Accuracy ($\pm 3\sigma$)
10,000	5.64E-6	0.0024	± 0.0071
15,000	3.76E-6	0.0019	± 0.0058
25,000	2.26E-6	0.0015	± 0.0045
30,000	1.88E-6	0.0014	± 0.0041

From these results, it was estimated that a set of 25,000 samples would give an acceptable value. However, in order to check the correctness of these estimations, a total of 8 sets of 25,000 samples were calculated. The probabilities derived from each set were then averaged and the statistical standard deviation was calculated, resulting in a value of $\sigma = 0.0010$ which is lower than the theoretical value of 0.0015 shown in Table 4. The average of these 8 values is $P_{ex} = \mathbf{0.0598}$ which is also an estimation of the exceedance probability obtained from a total of 200,000 samples. The estimated accuracy of this value is $\pm 3\sigma = \pm 0.0016$ with a confidence level of 99.7%. Therefore, the value $P_{ex} = \mathbf{0.0598 \pm 0.0016}$ can be considered a good approximation of the true value of the conditional exceedance probability to be compared with the results of the damage domain approach.

Integration in the damage domain

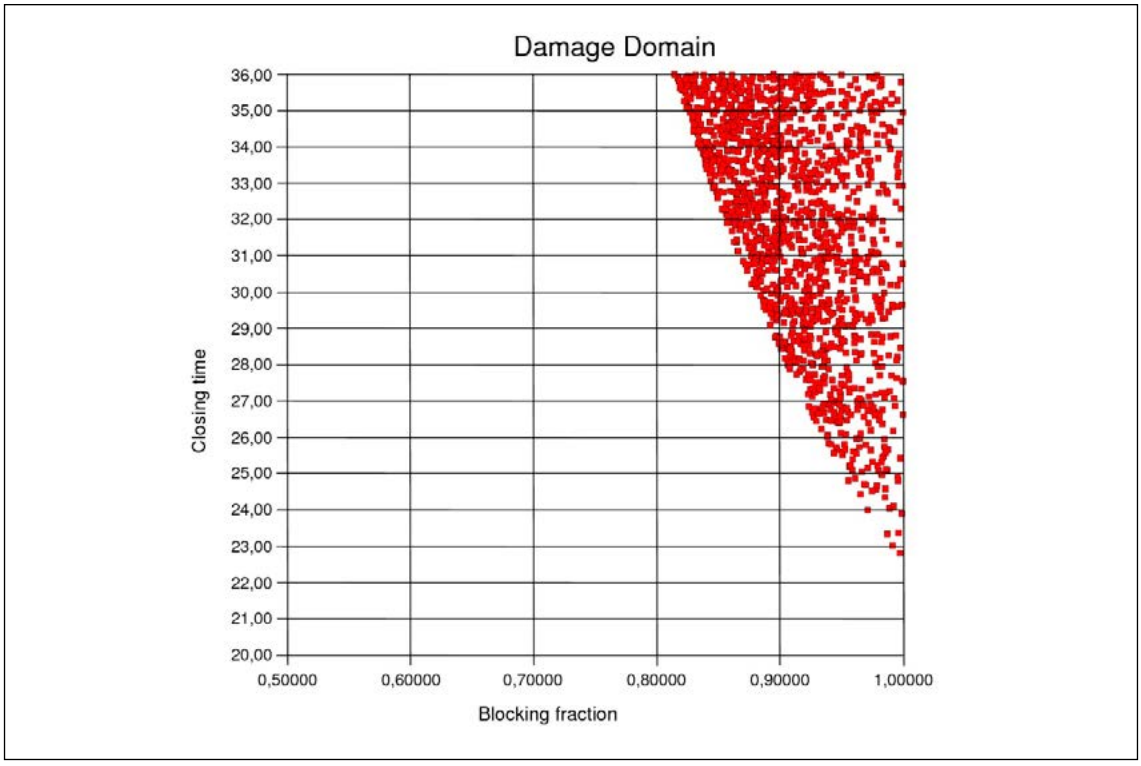
In a standard application of the damage domain approach, the first step would be the determination of the damage domain boundaries or, at least, of a region including it. For this purpose, a number of calculations should be performed. In this case, however, we have taken advantage of the results of the propagation approach. By labeling the samples resulting in limit exceedance we could determine with quite good accuracy the extension of the damage domain. The results are shown in Figure 18.

The probability density functions (*pdf*) of the uncertain parameters are in this case independent and the joint *pdf* of the two parameters is just the product of the two individual *pdf*s. The joint *pdf* needs

to be integrated over the damage domain in order to obtain the conditional probability of limit exceedance (tank overflow).

The integration method was the so-called *repeated one-dimensional integration* which consists of a nested scheme where each nesting level corresponds to one dimension of the integration space. This method can be extrapolated to any number of dimensions and, in most cases, produces more accurate results than Monte Carlo integration methods. For each dimension, a trapezoidal integration method has been applied, which is especially appropriated for smooth integrands.

Figure 18. Damage domain of the drain pipe blockage sequence (case 1)



Depending on the selected integration step for each dimension, the number of points which need to be evaluated will be different. Different combinations of integration steps have been tested and the results have been very similar, as could be expected from the exceptional smoothness of the integrand. The results are summarized in Table 5.

Table 5. Overflow probability results for different integration step sizes (case 1)

Bl. Frac. Step	Cl. Time step	No. of evaluated points	Cond. Ex. Prob.
0.01	0.1	1,568	0.0597
0.02	0.1	824	0.0594
0.01	0.2	822	0.0596
0.01	0.5	376	0.0592
0.01	1.0	225	0.0587
0.005	0.1	3,054	0.0598
0.03	1.0	83	0.0582
0.03	1.5	65	0.0576

It can be observed that all these results are very similar, practically insensitive to the sampling density, except for large integration steps and all of them (but the two last ones with largest integration steps in t_c) well within the interval 0.0598 ± 0.0016 determined as the best estimation of the exceedance probability from the propagation approach.

Conclusions of the automatic protection case

The main conclusion from this analysis case is that the two methods being compared produce equivalent results.

The number of points that need to be evaluated was much lower in the case of integration in the damage domain. However, this is not a general conclusion at all. Some particular characteristics of the problem made the damage domain approach especially efficient. Well delimited damage domains without long tails are particularly adequate for systematic sampling and numerical integration. This condition is necessarily matched when the uncertain parameters have a finite variability range as in this example.

A.3 2nd. Analysis case: manual protection with dynamic dependent distributions.

In this case we are going to consider uncertain times. The two protection actions are now executed by an operator. In practice, this means that the action is performed after an uncertain delay from the point where it is requested. In our case, actions are requested when the corresponding alarm signal is reached.

The alarm signals are, therefore, the respective stimuli of the protective actions. In our example, no deactivation mechanism is being considered. For each action, the probability distribution of the delay is not provided as a predefined function. Instead, an occurrence rate is defined for each stochastic event as a function of dynamic variables. These functions were determined in an arbitrary way without trying to represent any particular physical effect.

In order to partially compensate for the increase in complexity introduced by the consideration of two new uncertainties, the uncertainty of one of the parameters of the first analysis case was removed. Namely, the closing time of the feed valve is no longer uncertain and it was set to 20 seconds.

Therefore, the uncertainties considered in the second analysis case are the following:

Clogging fraction (S) of the normal drain pipe (size of the initiator) with the same probability distribution used in the first case.

Delay for PA1. Characterized by the following occurrence rate:

$$p_1 = \min\left[0.15\ , 0.02 \cdot \left(t - T_s^1\right)\right] + 15\frac{dl}{dt} + 0.1 \cdot l^2 \tag{A-5}$$

Delay for PA2. Characterized by the following occurrence rate:

$$p_2 = \min\left[0.2\ , 0.04 \cdot \left(t - T_s^2\right)\right] + 50\frac{dl}{dt} + 0.4 \cdot l^2 \tag{A-6}$$

with T_s^1 and T_s^2 being the activation times of the high and high-high level alarms, respectively and l being the tank level.

Propagation of input uncertainties

The main difficulty for applying the propagation method based on random sampling of the uncertain items is that only the distribution of the parameter $\underset{\sim}{}$ is provided as problem data. Delay times, characterized only by occurrence rates, cannot be sampled before the simulation.

In order to deal with this difficulty, two methods were proposed and tested for obtaining a set of randomly selected transients suitable for statistical estimation of the overflow probability. These methods are discussed below.

Sampling method 1: building-up the probability distribution

The first method consists of emulating the usual sampling method for known probability distributions. This method requires the computation of the probability distribution during the simulation of the plant transient. Using the assumed function for the occurrence rate and the second relation of equation (A-2), the cumulative probability function $F(t)$ can be calculated as an additional simulation variable. Note that, before the activation of the corresponding stimulus, both $p(t)$ and $F(t)$ are null.

For each uncertain time, a random number R in the $[0,1]$ interval is selected before the simulation. At some time point, the stimulus of the event is activated and the function $F(t)$ starts growing. Then, the occurrence of the event is delayed until the condition $R=F(t)$ is met and the event is forced to occur at that point.

As in the previous case, several sets of different number of samples have been calculated. From these calculations it was found that the overflow probability in this case would be in the neighborhood of 0.173. For this probability value, the expected accuracy as a function of the number of samples is shown in Table 6.

Table 6. Expected accuracy of the overflow probability (case 2)

No. of samples	Variance	σ	Accuracy ($\pm 3\sigma$)
10,000	1.4273E-5	0.00378	± 0.0113
15,000	9.5156E-6	0.00308	± 0.0093
25,000	5.7094E-6	0.00239	± 0.0072
30,000	4.7578E-6	0.00218	± 0.0065

The results of the calculation of eight sets of 25,000 samples resulted in an average of $P_{ex} =$ 0,17249 with a statistical standard deviation of 0,00199, lower that the theoretical value 0,00239. The $\pm 3\sigma$ accuracy of the average value, when considered as the result of the calculation of a set of 200,000 samples can be estimated as $\pm$0,0025. Therefore, the value of $P_{ex} =$ **0.17249** $\pm$**0.0025** is a good estimation of the overflow probability to be compared later with results from alternative methods.

A main question about the validity of this method aroused from the fact that a different probability distribution is being sampled for each transient. The question was then whether the resulting sample of the output variable was adequate for calculating the exceedance probability.

Given the practical character of this exercise, no attempt was done to answer this question in a general and rigorous way. As will be shown later, the results suggest that this is a valid method but this is only an observation from a particular case.

Sampling method 2: decision at time step level

In the second method the decision on when the event is going to occur during a simulation is directly based on the occurrence rate. Neither the *pdf* nor the *cdf* need to be calculated along the transient.

Taking into account that the occurrence rate $p(t)$ is the probability of occurrence per unit time at differential level, the probability of occurrence of an event i during a small time interval can be approximated by $P_i(\Delta t) = p(t) \cdot \Delta t$. In this sampling method, a random number in the interval $[0,1]$ is generated at each time step for each event with active stimulus. The random number is compared with $P_i(\Delta t)$. If the random number is lower than the probability, the event id forced to occur. If not, the simulation continues without the occurrence of the event.

The overflow probability is calculated, as in the other cases of propagation based on random sampling, as the ratio between damage transients and total number of simulated transients. Considerations about accuracy as a function of the number of samples are identical to the first sampling method.

Using this sampling method, eight values of overflow probability were calculated, each one based on the simulation of 25,000 transients as in the previous sampling method. The average of these eight values was **0,17282** with a statistical standard deviation of 0,00217. This average is nearly identical to the one resulting from the first sampling method.

Integration in the damage domain

Uncertain times associated to protective actions have a particularly useful characteristic for the application of the damage domain approach. When the remaining conditions do not change, enlarging the delay of a particular event has an adverse effect on safety and moves the system state closer to the damage condition. This allows for a very systematic procedure to identify and travel through the damage domain while integrating the probability density function.

Let us consider the example of the tank system and let us for now reduce the problem to two dimensions by fixing the value of the blocking fraction in drain clogging events. When the water level reaches the first alarm level as a consequence of the initiating event, it is necessary to perform the first protective action. Otherwise, the level will continue increasing and getting closer to the overflow condition. The same occurs when the second alarm level is reached and the second protective action is required. It is clear that, if none of the actions is performed, the tank overflow will occur for sure.

Taking into account that protection delays beyond the occurrence of the overflow are worthless, the transient with no protective action performed is a well defined boundary of the damage domain. As indicated in the concluding remarks of the 1st analysis case, this is a favorable condition for the application of the damage domain approach using the repeated 1-D integration method in a systematic way.

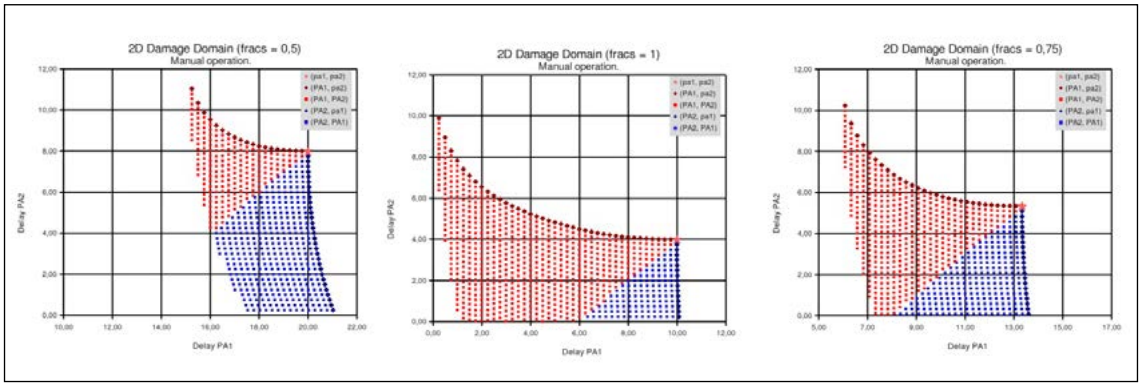
Since there are three uncertain elements involved, the damage domain is three-dimensional and, therefore, difficult to draw. However, by taking a fixed value for the clogging fraction we can get a 2-D section of the damage domain. Three of these sections have been represented in Figure 19, corresponding to different values of the clogging fraction s. As indicated in the legend, these graphs actually represent damage domains of several dynamic sequences:

- The sequence without protective actions is represented by a single star point in each 2-D graph.

- Diamonds represent the damage domains of sequences with only one protective action: red diamonds when only PA1 occurs and blue diamonds when only PA2 occurs.
- Red squares describe the damage domain of the sequence where PA1 occurs before PA2 while blue squares correspond to the sequence where these two events occur in reversed order.

As in the previous case, a search for optimal integration steps was performed before the final calculation. Two-dimensional calculations, with fixed values of the parameter s were first performed in order to find the optimal integration steps for uncertain times. Two values of s, relatively near the extremes of the variation interval were used. For $s = 0.6$, an adequate balance between proximity to the convergence value and number of calculations was found for time steps of both delays equal to 0.3 seconds. However, for $s = 0.9$, the most convenient integration steps were 0.5 seconds for the occurrence of PA1 and 0.2 for the occurrence of PA2. In both cases, however, a relatively low sensitivity to the integration step sizes and the existence of a convergence value, were observed.

Figure 19. Damage domain of the manual protection case



Optimizing the time integration steps for each value of the parameter would be possible. However, it was considered more convenient to use the same values of the time integration steps for any value of s. It was then decided to use 0.4 seconds as the integration step for both uncertain times. The determination of the optimal integration step for s was done in a similar way and the results are shown in Table 7.

Table 7. 2nd. analysis case: Overflow probability results for different integration steps of s .

S step	t^1 step	t^2 step	No. of simulations	No. of damage cases	Overflow probab.
0.01	0.4	0.4	20,651	19,296	0.1740
0.02	0.4	0.4	10,542	9,842	0.1739
0.03	0.4	0.4	7,301	6,801	0.1736
0.04	0.4	0.4	5,643	5,250	0.1732
0.05	0.4	0.4	4,484	4,175	0.1727
0.06	0.4	0.4	4,067	3,763	0.1721
0.07	0.4	0.4	3,621	3,351	0.1711
0.08	0.4	0.4	3,225	2,975	0.1726
0.04	0.1	0.1	67,722	66,505	0.1706

The fifth row of Table 7, with an overflow probability of 0.1727, was selected as the most balanced calculation, taking into account the proximity to the convergence value and the number of simulations. Nevertheless, it can be seen that all the results in Table 7 are well within the 99.7% confidence interval calculated from the random sampling methods

Conclusions of the manual protection case

The main conclusion from this analysis case is that, as in the case of automatic protection, both methods produce equivalent results. Moreover, the two random sampling methods that have been devised for cases with dynamic dependences have been found equivalent. Therefore, the selection of one method or the other can be exclusively based on efficiency aspects.

When uncertain times of protective actions are present in the problem, the main advantage for the damage domain approach can be taken from the fact that the production of the damage condition (tank overflow) is an absolute limit for the execution of those actions. Once the damage has been produced, it does not make sense to consider later execution of protective actions intended to avoid that damage. This allows for a very systematic method for identifying the damage domain while the probability density function is being integrated. This method also helps avoiding the simulation of useless transients.

A.4 Overall conclusions of the exercise

This application exercise was developed with the purpose of comparing different approaches to the uncertainty analysis. The exercise has not been exhaustive. Only simple random sampling has been applied for propagation methods because this has been considered the most general propagation approach. Other techniques like stratified or biased sampling are considered approximations or particular cases of the general approach and have not been included. Similarly, only repeated 1-D integration has been used for the damage domain approach. Other integration methods that could be more efficient in some cases but are less general have been left out of the scope of the work.

All the conclusions of this work should be considered as preliminary results. These conclusions are just observations derived from the analyzed cases but a formal generalization and/or delimitation of the conditions for validity has not been tried.

The main conclusion is that the propagation and the damage domain approaches are equivalent in all the cases that have been analyzed. The two approaches can be understood as dual techniques. Usual propagation methods perform a forward propagation of data uncertainties to output variables where the damage domain is well defined while the damage domain approach consists of a back-propagation of the output damage domain to the space of the problem data.

The equivalence between the two approaches depends on a proper application of the respective methodologies. In particular, random sampling of uncertain times can be done only when the corresponding probability distribution is known. The most important practical consequence is that, when dynamic dependencies are present, the simulation cases cannot be decided in advance, as in standard applications of BEPU methodologies. It is only during the simulation when the dynamic dependent uncertain times can be characterized and, therefore, properly sampled.

In the application of the damage domain method, the number of transients that need to be simulated depends on several factors. One of them is the sharpness or smoothness of the probability distributions, which conditions the sampling density in each dimension. Another one is the integration method that should provide a good balance between accuracy and simplicity. Even if the repeated 1-D integration is used as a very general integration procedure, different levels of sophistication can be applied for each dimension in order to optimize the number of points to be calculated.

Other than that, random sampling of dynamically dependent uncertain times can be done either at integral or differential level. In the first case, the probability distribution is built along the transient until a pre-selected random decision criterion is reached. In the second case the short term occurrence

probability, i.e., the probability of occurrence during a simulation time step, is compared with a random decision criterion which is redefined at every time step.

The main advantage of the damage domain approach is that it allows focusing on the area where damages are generated. This is the area of interest for safety analyses. The identification of the damage domain boundaries may require the calculation of some non-damage transients but, in general the great majority of the simulated transients are damage transients. However, the number of required simulations ``explodes`` as the number of uncertain elements grows. The damage domain approach is more recommendable when the number of uncertain items is small and the damage domain is a small fraction of the uncertainty space. It has also clear advantages when the boundaries of the damage domain can be easily identified.

On the other hand, the random sampling based propagation approach is not sensitive to the number of uncertain elements. However, the number of simulated transients required to get a given level of accuracy is usually high. Moreover, the number of non-damage simulated transients can be very high, especially in the most desirable case of small damage domains. The random sampling propagation approach is more convenient when the number of uncertain items is high and when the damage domain covers a significant fraction of the uncertainty space.

Taking into account the advantages of each method, a combined approach could result in an optimum balance between effort and accuracy. Using random sampling propagation for uncertain model parameters and damage domain for uncertain times can result in an optimum method for exceedance probability calculations. Some methods of this type are being explored.

References

References

[1] Task Group on Safety Margins Action Plan (SMAP). Summary record of the meeting of an ad-hoc group of experts to discuss further a CSNI Action Plan in the area of safety margins. NEA/SEN/SIN/SMAP(2003)1. 12-Sep-2003.

[2] Task Group on Safety Margins Action Plan (SMAP). Safety Margins Action Plan. Final Report. NEA/CSNI/R(2007)9. Nuclear Energy Agency, 2007. http://www.oecd-nea.org/html/nsd/docs/2007/csni-r2007-9.pdf

[3] NEA Report, Safety Margin Evaluation - SMAP Framework Assessment and Application. NEA/CSNI/R(2011)3. http://www.oecd-nea.org/nsd/docs/2011/csni-r2011-3.pdf.

[4] Adolfsson, Y., Holmberg, J.E., Hultqvist, G., Kudinov, P., Männistö, I. Proceedings of the IDPSA-2011, Proceedings of the "Deterministic/Probabilistic Safety Analysis Workshop», October 2011. http://www.vtt.fi/inf/julkaisut/muut/2011/VTT-R-07266-11.pdf.

[5] Adolfsson, Y., Holmberg, J.E., Karanta, I., Kudinov, P., Proceedings of the IDPSA-2012. Integrated Deterministic-Probabilistic Safety Analysis Workshop, November 2012. http://www.vtt.fi/inf/julkaisut/muut/2012/VTT-R-08589.pdf.

[6] Kudinov P., Vorobyev Y., Sánchez M., Queral C., Jiménez G., Rebollo M.J., Integrated Deterministic-Probabilistic Safety Assessment Methodologies, Nuclear Esp 2014;347:32-8, January 2014.

[7] Di Maio, F., Zio, E., Smith, C., Rychkov, V., Integrated deterministic and probabilistic safety analysis for safety assessment of nuclear power plants. Sci. Technol. Nucl. Installations 2015 (special issue), http://refhub.elsevier.com/S0306-4549(16)30557-6/h0165

[8] Szilard. R., Zhang H., Epiney A, TU L., R&D Plan for RISMC Industry Application #1: ECCS/LOCA Cladding Acceptance Criteria, INL/EXT-16-38231, April 2106, https://lwrs.inl.gov/SitePages/Reports.aspx

[9] Mandelli D. et al., Data Analysis Approaches for the Risk-Informed Safety Margins Characterization Toolkit, INL/EXT-16-39851, September 2106, https://lwrs.inl.gov/SitePages/Reports.aspx

[10] Hess S. et al., Framework for Risk-Informed Safety Margin Characterization, EPRI, Palo Alto, CA: 2009. 1019206, Final Report, December 2009.

[11] Hess S. et al., Technical Framework for Management of Safety Margins—Loss of Main Feedwater Pilot Application. EPRI, Palo Alto, CA: 2011. 1023032, Final Report, November 2011.

[12] Izquierdo, J. et al., An Integrated PSA Approach to Independent Regulatory Evaluations of Nuclear Safety Assessments of Spanish Nuclear Power Stations. EUROSAFE forum, Paris, 2003.

[13] Izquierdo Rocha, J.M. et al., CSN Experience in the Development and Application of a Computer Platform to Verify Consistency of Deterministic and Probabilistic Licensing Safety Cases. Volume I: General Approach and Deterministic Developments, Colección Otros Documentos CSN. ODE-04-22, September, 2016, https://www.csn.es/centro-de-documentacion

[14] Izquierdo Rocha, J.M. et al., The Importance of Accident Time Evolution in Regulatory Safety Assessment. Independent, Quantitative Tools and Methods at CSN to Ensure Adequate PSA/DSA Applications. Deterministic Aspects, Colección Otros Documentos CSN, ODE-XX-YY, December, 2016, https://www.csn.es/centro-de-documentacion

[15] Herrero R., A Standardized Methodology for the Linkage of Computer Codes. Application to RELAP5/Mod3.2, NUREG/IA-0179. US Nuclear Regulatory Commission. Office of Nuclear Regulatory Research.

[16] Ibañez L. et al., Application of the Integrated Safety Assessment Methodology to Safety Margins. Dynamic Event Trees, Path Analysis and Risk Assessment, Reliability Engineering & System Safety (2015), http://dx.doi.org/10.1016/j.ress.2015.05.016i.

[17] Sattison M.B., Hall K.W., Analysis of Core Damage Frequency: Zion, Unit 1 Internal Events. NUREG/CR 4550 vol. 7 rev.1, Idaho National Engineering Laboratory. Prepared for the US Nuclear Regulatory Commission. May 1990.

[18] Izquierdo, J.M., Cañamon, I., Status report on dynamic reliability: SDTPD path and sequence TSD developments. Application to the WP5.3 benchmark Level 2 PSA exercise. DSR/SAGR/FT 2004.074, SARNET PSA2 D73 (rev.1). 2006.

[19] Izquierdo J.M., Cañamón I., TSD, a SCAIS Suitable Variant of the SDTPD, Presented at ESREL-2008 & 17th SRA Europe Annual Conference, Valencia (Spain), September, 2008.

[20] Sancaktar S., WOG 2000 Reactor Coolant Pump Seal Leakage Model for Westinghouse PWRs. WCAP 15603 rev.1-A. Westinghouse Electric Company LLC. June 2003.

[21] Brookhaven National Laboratory, Guidance Document for Modeling of RCP Seal Failures, W9611-0899, August 1999.

[22] Scientech Inc., Cost/Benefit Analysis for Generic Issue 23: Reactor Coolant Pump Seal Failure, NUREG/CR-5167, April, 1991.

[23] Westinghouse Owners Group, Reactor Coolant Pump Seal Performance for Appendix R Assessments. WCAP-16396-NP, January 2005.

[24] N. de los Santos, Efficient Algorithms for Dynamic Probabilistic Safety Assessment. An Application to Convex Damage Domain, Thesis for the degree of Master of Advanced Computing for Science and Engineering, UPM, Madrid, September 2011.

[25] N. de los Santos, Risk Assessment Tool. APSRIT Project (CSN/UPM), PSA Advanced Methods for Technology Independent Regulation, APSRIT/IT-01/0710 (ver 1), Madrid, July 2010. (in Spanish)

The Problem of Safety Margin Assessment within the Risk-Informed Regulation

Colección
Otros Documentos CSN

CSN CONSEJO DE SEGURIDAD NUCLEAR