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

Colección
Otros Documentos
40.2016

CSN CONSEJO DE SEGURIDAD NUCLEAR

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

J. M. Izquierdo Rocha, J. Hortal Reymundo, M. Sánchez Perea, E. Meléndez Asensio
Modeling and Simulation Area, Nuclear Safety Council of Spain

CSN CONSEJO DE SEGURIDAD NUCLEAR

Colección
Otros documentos CSN
Referencia: ODE-04.22

Publicado y distribuído por:
Consejo de Seguridad Nuclear
Justo Dorado, 11. 28040 - Madrid
http://www.csn.es
peticiones@csn.es

Maquetación: Tau Diseño
Depósito legal: M-10851-2016

Contents

Resumen Ejecutivo

Resumen ejecutivo

Las tareas propias de un Organismo Regulador, y por tanto del CSN, son específicas y distintas de otras 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.

Esta publicación revisa las actividades del area MOSI del CSN en el desarrollo y aplicación de una plataforma computacional que ayude en la verificación de la consistencia cruzada de los análisis de seguridad de plantas nucleares basadas en las aproximaciones determinista y probabilista. Su motivación nace del contexto anterior.

Globalmente el trabajo se divide en dos volúmenes. El presente Volumen I describe la metodología ISA (Análisis Integrado de Seguridad) propuesta desde MOSI, así como la plataforma computacional SCAIS (Sistema de Códigos de Simulación para el Análisis Integrado de Seguridad) asociada, con mayor énfasis en ambos casos en los aspectos deterministas del problema de la seguridad.

En el Volumen II se describirán con mayor detalle los aspectos probabilistas de la metodología y los problemas asociados a la cuantificación del riesgo. También se incluirá en dicho volumen la descripción de técnicas computacionales avanzadas que mejoran significativamente la eficacia de la metodología ISA haciendo más práctica su aplicación.

Los desarrollos y actividades descritos en este Volumen I han sido realizados 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).

El primer capítulo desarrolla en detalle las implicaciones de la motivación aludida, incluida la necesidad de abordar las tareas de licenciamiento de instalaciones nucleares con fundamentos sólidos acordes con la importancia del problema, implicaciones que han dado lugar a los trabajos que se describen en el resto del documento.

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 Capítulo II describe el proceso histórico por el que el área MOSI y sus grupos predecesores han ido desarrollando distintos elementos metodológicos y computacionales que han dado lugar a la metodología ISA y a la plataforma SCAIS 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 desarrollos a nivel internacional.

El desarrollo de herramientas de simulación ha ido cubriendo sucesivamente aspectos de operación normal, accidentes con fenomenología bifásica, accidentes severos y actuaciones de los operadores. Simultáneamente se ha ido desarrollando 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 desarrollando 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.

En el Capítulo III se aborda la comparación entre los enfoques existentes. En primer lugar se hace un repaso de conceptos fundamentales que se utilizan en los distintos tipos de análisis.

Se intenta precisar las definiciones e identificar las implicaciones que su uso tiene en las distintas aplicaciones. Algunos de estos conceptos están presentes en diversas metodologías mientras que otros han nacido en el contexto de un tipo concreto. Sin embargo, una comprensión adecuada de estos conceptos permite identificar mejor las capacidades y las limitaciones de cada método.

Algunos de estos conceptos han sido y siguen siendo de uso común en el territorio de los análisis de seguridad, como el de barrera protectora, límite de seguridad o envolvente de seguridad, aunque en algunos casos su uso repetido puede haber dado lugar a que se desvirtúen. Otros pueden considerarse como novedosos aunque en realidad han estado implícitamente presentes y con frecuencia inadecuadamente tratados en las metodologías tradicionales. Este es el caso de los conceptos de estímulo (puntos de ajuste de los sistemas de protección automáticos, condiciones de entrada en procedimientos de emergencia y en general condiciones necesarias para la toma de decisiones), o de dominio de fallo/daño de los que se hace uso explícito en la metodología ISA de MOSI y en otras metodologías integradas.

El resto del Capítulo III se dedica a discutir la forma en que los distintos tipos de metodologías, concretamente DSA, PSA e ISA aplican los conceptos antes aludidos y en consecuencia cual es el campo natural de aplicación de cada tipo. Un matiz que conviene destacar es que la calificación de una metodología como determinista, probabilista o integrada no significa que no estén siempre presentes ambos aspectos del problema aunque el énfasis o la visibilidad se pongan principalmente en el lado determinista (DSA), en el probabilista (PSA) o en ambos a la vez (ISA).

El Capítulo IV describe la plataforma computacional SCAIS que materializa los principios teóricos de la metodología ISA en un conjunto de herramientas para su aplicación práctica. Se describen los distintos elementos que componen SCAIS, poniendo el énfasis en aquellos módulos que desarrollan las capacidades de análisis deterministas y dejando para el Volumen II una descripción más detallada de los módulos probabilistas.

La característica más destacada de SCAIS en su vertiente determinista es la capacidad para generar de forma automática árboles de sucesos dinámicos, es decir, conjuntos de simulaciones en forma de árbol en los que la posibilidad de ocurrencia o no de determinados sucesos significativos da lugar al nacimiento de nuevas ramas de dicho árbol. Para el desarrollo de esta capacidad es fundamental disponer por una parte de los modelos de simulación adecuados y por otra de un módulo de gestión de la simulación capaz de organizar adecuadamente el despliegue del árbol y de recoger la gran cantidad de información generada.

El "motor de simulación" BABIECA permite construir modelos de simulación de todo tipo de alcance y nivel de detalle a partir de módulos internos o de códigos externos que se hayan adaptado para su acoplamiento al sistema. Códigos como MAAP o RELAP5 ya se han adaptado y pueden ser utilizados como módulos de BABIECA. Otros como TRACE o MELCOR podrán ser adaptados en el futuro. El uso de códigos externos a través de BABIECA permite utilizar sus resultados como si dichos códigos funcionaran de forma autónoma pero también

permite complementar los modelos de dichos códigos con módulos internos de BABIECA que ofrecen la posibilidad de construir nuevos elementos de control, obtener información adicional mediante el post-proceso de resultados, etc. También se pueden construir modelos completos utilizando exclusivamente módulos de BABIECA. Estas características otorgan al sistema una gran flexibilidad.

Un caso particular de código externo con capacidad de acoplamiento a BABIECA es el simulador de procedimientos SIMPROC que permite simular la ejecución de los procedimientos de operación teniendo en cuenta el estado de la planta en cada momento.

El módulo que se encarga de la gestión de las simulaciones en árbol es DENDROS que tiene capacidad para iniciar nuevas simulaciones utilizando criterios de ramificación definidos por el usuario y optimizando los recursos para que no se repitan partes de la simulación ya calculadas. Además, DENDROS genera las demandas de cuantificación probabilista para que los módulos correspondientes proporciones la información que pueda resultar necesaria durante el proceso de despliegue del árbol de simulación.

Otros módulos de SCAIS se encargan de la identificación de dominios de fallo/daño de las secuencias del árbol y de la cuantificación del riesgo. Además, un elemento fundamental es una base de datos donde se recoge, organiza y conserva toda la información de entrada y de salida de cada uno de los casos de análisis. Esto permite, entre otras cosas, la reutilización de dichos datos para análisis posteriores sin necesidad de repetir todas las simulaciones.

En el Capítulo V se hace una recopilación de las capacidades de la metodología ISA para abordar aspectos concretos de los análisis de seguridad. En este Volumen I se discuten solamente las capacidades para analizar aspectos deterministas mientras que en el Volumen II se ampliará esta discusión a los aspectos probabilistas y a aquellos que requieren un planteamiento conjunto.

Una característica fundamental del DSA es la definición y utilización de una Envuelta Base de Diseño (DBE en sus siglas en inglés) compuesta por el conjunto de transitorios base de diseño que son objeto de análisis. Tradicionalmente, la verificación del DSA se ha centrado de manera muy preferente en la comprobación de que los resultados del análisis de dichos transitorios cumplen con los criterios de aceptación establecidos. Sin embargo, se ha prestado mucha menos atención al problema, mucho más complejo pero fundamental, de verificación de la envolvente, es decir, la comprobación de que el conjunto de transitorios base de diseño analizados configuran realmente una envolvente de seguridad. En este documento se discuten las capacidades que ofrece la metodología ISA para abordar la verificación de la DBE.

Como se ha indicado anteriormente, aunque el PSA se considera una metodología probabilista, contiene aspectos deterministas de importancia capital. Uno de ellos es la delineación de secuencias en sus árboles de sucesos. La decisión de incluir puntos de ramificación bajo un determinado cabecero depende de que la función de seguridad representada por el cabecero haya sido realmente demandada o no, cuestión que es netamente determinista. Incluir un punto de ramificación espúreo o ignorar un punto de ramificación real da lugar a cuantificaciones erróneas

que pueden ocultar problemas de seguridad. La metodología ISA proporciona medios para abordar este problema.

Otro aspecto netamente determinista de las metodologías de PSA en su Nivel 1 es la definición de criterios de éxito de sistemas y de funciones de seguridad. En el documento se discute como estos criterios de éxito se determinan mediante métodos que son en realidad una extensión del DSA y que tiene mucha relación con la verificación de envolventes antes mencionada. Por tanto, la metodología ISA también permite abordar la verificación de criterios de éxito en el PSA de Nivel 1, que es una de las bases fundamentales del PSA.

La verificación de procedimientos de operación de emergencia es otro de los campos de aplicación de la metodología ISA en el contexto del APS de Nivel 1 donde habitualmente se modelan las principales acciones de estos procedimientos.

En el Capítulo VI se hace una breve presentación de varios ejemplos de aplicación que se han realizado desde el inicio del desarrollo de la metodología.

Históricamente, la primera aplicación se hizo para el estudio de los procedimientos de operación de emergencia previstos para el accidente de rotura de tubos del generador de vapor en la C.N. José Cabrera que, como es sabido, disponía de un único generador de vapor, lo que hacía que este accidente tuviera características singulares en esta planta.

El segundo ejemplo presentado, relativo también al accidente de rotura de tubos en generadores de vapor pero en una planta de tres lazos, muestra la capacidad de la metodología para utilizar criterios de éxito de secuencias distintos de los tradicionales del PSA. De esta forma se pueden analizar impactos radiológicos significativos en accidentes no incluidos en la base de diseño pero que no implican la degradación severa del núcleo.

El tercer ejemplo ilustra el uso de la metodología ISA para el estudio del impacto en los márgenes de seguridad de cambios significativos en el diseño o en la operación de las plantas. Este ejemplo describe la contribución del área MOSI al Grupo de Trabajo SM2A de la NEA en el que se realizó una aplicación de los principios metodológicos desarrollados previamente en el Plan de Acción sobre Márgenes de Seguridad (SMAP), también en el marco de la NEA.

Otro ejemplo de aplicación muestra el uso de la metodología para el análisis de distintos aspectos de accidentes de tipo LOCA en función del tamaño de la rotura y del tiempo que los operadores tardan en iniciar la despresurización manual requerida por los procedimientos.

Por último, se muestra un ejemplo en el que se valora bajo qué circunstancias puede ser adecuada una medida concreta requerida en los procedimientos de operación de emergencia y en las guías de accidente severo. En concreto se trata del disparo de las bombas principales de un PWR en accidentes con roturas pequeñas en los que, tras una pérdida del sistema de inyección de alta presión, este sistema vuelve a recuperarse. Se discuten diversas posibilidades y se muestra el impacto que cada una de ellas tendría en las consecuencias del accidente.

Entre las conclusiones más significativas (en particular relativas a los importantes problemas 1 y 2 anteriores, y que son cruciales para la discriminación de la calidad), están que

tanto la delineación de los arboles del PSA nivel 1 como la verificación del DSA son dependientes del diseño de estímulos, y que cambios en ellos requieren revisión de los análisis y de sus conclusiones.

El Volumen II tratará más ampliamente las dificultades que estas conclusiones plantean a la consistencia de análisis probabilistas y deterministas. Dada su complejidad, los aspectos técnicos más especializados que están en la base de la solución que se propone en MOSI, son objeto de otra publicación separada.

Abstract

This contribution reviews CSN/MOSI activities in the development and application of a computer platform to verify consistency of deterministic and probabilistic licensing safety cases. It is divided in two Volumes. The present Volume I describes the MOSI Integrated Safety Assessment methodology (ISA), and details/justifies some of the MOSI activities in the deterministic side. Volume II will summarize more advanced methods and provide similar information in the probabilistic side.

The computer platform for ISA implementation SCAIS (Simulation Code System for Integrated Safety Assessment) is also briefly summarized with due references. The following topics are included:

- Theoretical developments;
- Developmental tools;
- Platform features;
- Integrated computer codes;
- Pilot applications and participation in international activities; and
- Examples of licensing applications.

I. Introduction. Potential Benefits of Computerized, Diagnostic Tools for Verification of Industry Safety Assessments

I. Introduction. Potential Benefits of Computerized, Diagnostic Tools for Verification of Industry Safety Assessments

I.1. On the Need of Diagnostic Tools

Most often, in defending their safety cases within the licensing process, industry safety analyses have to rely on computational tools and methods including Deterministic (DSA) and Probabilistic (PSA) Safety Assessments. Such an assessment capability, even if reduced to its analytical aspects, is a huge effort requiring considerable resources.

The increasing trend towards Risk Informed Regulation (RIR) motivates an even larger demand for computerized safety case analysis. It has been further fostered by:

- New nuclear power plant designs;
- The large time span and evolution of the old "generic" safety analysis, that requires confirmation of its present applicability;
- The need to extend the life, to increase the power or to implement significant design modifications of the existing plants with associated challenges in terms of potential reduction in their safety margins, and
- The need to consider severe accident scenarios.

This complex situation generates a parallel need in regulatory bodies that makes it mandatory to increase their technical expertise and capabilities in this area. Together with regulatory bodies, Technical Support Organizations (TSOs) have become an essential element of the regulatory process, providing a substantial portion of its technical and scientific basis via computerized safety analyses supported on available knowledge and analytical methods/tools.

Regulatory/TSO support activities cannot have the same scope as their industry counterparts, nor is it reasonable to expect the same level of resources. Moreover, in a general case, regulators and TSOs need to assess licensing applications for a variety of different technologies and the optimization of resources has raised the interest in methods that are technology neutral (see [1], [2]). In providing its technical expertise, they shall:

- Review and approve methods and results of licensees, and
- Perform their own analysis/calculations to verify the quality, consistency, and conclusions of day to day industry assessments.

The latter is a difficult, different and very special regulatory task, requiring specific diagnostic tools to independently check the validity and consistency of the many assumptions used and conclusions obtained by the licensees in their safety assessments. They are essential for efficient use of their resources and ought to be adequate to the usually smaller size of the regulatory body. Efficiency is enhanced by increasing the international cooperation among national organizations to jointly develop tools and methods independent on domestic technology that may then be customized to their plants.

The approach shall include a sound combination of deterministic and probabilistic checks, complementary pieces however of an integral safety assessment method, so that they constitute a comprehensive sample verifying all relevant decision making risk factors and ensuring that these decision ingredients are properly and consistently weighted ([3], [4], [5]).

I.2. Problems of Particular Relevance

Typically, supporting analyses presented by the licensees are qualified as deterministic or probabilistic depending on whether they focus on verification of design basis safety margins or on reliability issues and estimation/quantification of some risk indicators. These two types of analysis are recognized as complementary although they are usually performed in a separate manner even if some mutual influences are identified and taken into account. There are, however, some issues that require an integrated approach where the two types of analysis are closely combined.

More precisely, in the regulatory side, some issues that require an integrated approach and a systematic set of checks arise when considering:

- The process by which the insights from these complementary safety analyses are combined, and
- Their relationships when addressing high level requirements such as defense in depth and safety margins.

Important sources of practical examples are the analyses justifying the PSA success criteria and operating technical specifications (see Section III below) and their mutual consistency. Frequently, they are still supported by potentially outdated base calculations made in older times in a different context and with other spectrum of applications in mind. They are but important chapters of the optimization of the protection system design encompassing, for instance, problems like:

- Ensuring that the protection system is able to cope with all accident scenarios and not only with a predetermined set. This umbrella character is hard to prove, particularly within an atmosphere of reduced safety margins. It requires careful regulatory attention to the historic evolution of the Deterministic Safety Assessments (DSA), and it is a source of potential conflicts when risk techniques are involved in the regulatory process.
- Ensuring the umbrella condition of PSA success criteria, which become critical and sensitive. Extension to operator actions of the automatic protection design is a source of potential inconsistencies involving complex aspects like available times for operator action. Verification of Emergency Operating Procedures (EOPs) is also worth mentioning, because it implies accident time scales longer than those considered in the automatic design and important uncertainties in the timing and conditions of interventions, both potentially altering the umbrella character of the deterministic design.

- Allowing the necessary extension of the scope of the analysis because of the need to consider degraded core situations to ensure acceptable residual risks. Again, consistency issues appear requiring regulatory checks.

These consistency checks call for an appropriate extension of the probabilistic safety metrics used. Different exceedance frequency limits for different barrier safety limit indicators have been extensively discussed and may be used as a sound risk domain interpretation of the existing regulations (see [6]). For instance, frequency limits for partial core damage or few core fuel failures may correctly interpret the present deterministic rules for safety margins in a way consistent with a probabilistic approach.

All this, in turn, has implications on the bases of the operating technical specifications, derived from those analyses which so much affect the daily regulatory plant life and go beyond the licensing activities during the design phase.

Together with design related checks, there is also room for improvements in the analysis of operating events and their associated lessons learned by putting the correct focus on the many aspects discussed above. This way, consistency between analysis assumptions and real plant behavior can be confirmed or not in real life incidents. Most incident analysis approaches currently focus almost exclusively on safety metrics derived from event tree-fault tree quantifications, such as severe core damage frequency (CDF) and large early release frequency (LERF) which provide only a partial view of the incident implications.

I.3. CSN Developments: an Example of Diagnostic Tools and Verification Methods

Just as an example of already existing projects in this direction, the area of Modeling and Simulation (MOSI) of CSN has developed its own Integrated Safety Assessment (ISA) methodology for this purpose (see [7]). This diagnostic method has been designed as a regulatory tool, able to compute the exceedance frequencies of accident sequences and to check in an independent way the results and assumptions of the industry PSAs, including their RIR extensions/applications, as well as those of the deterministic analysis. The approach harmonizes the probabilistic and deterministic safety assessment aspects via a consistent, unified and suitable computational simulation framework called SCAIS.

In the sequel, this document summarizes the work done at CSN to establish this integrated approach implemented in a simulation framework for independent assessment of safety studies. The document will elaborate on the following points:

1. A brief survey of past work. The effort was devoted to assimilate DSA methods, to perform independent studies oriented to understand current PSA practice and to develop methods to assess licensing issues of Spanish Nuclear Power Plants. It will touch upon the theoretical framework that guided the approach.
2. Main features of old and new developments to synthesize a simulation package able to independently verify and/or reproduce portions of a PSA or a DSA with the aim of its regulatory evaluation.

3. Steps done in the development of the Integrated Safety Assessment software package and methodology used at present by the Area of Modeling and Simulation at CSN. These software tools and methods allow for addressing quantitatively:
   a. the simulation of the time evolution of plant states in trees of nuclear accident sequences resulting from exploring potential equipment degradations subsequent to initiating events,
   b. the simulation of operator actions, and their interaction with the plant state, and
   c. the sequence probability calculations and risk integration.
4. Recent applications of the method and tools to different purposes:
   a. Assessment of completeness of Event Tree delineation;
   b. Verification of Emergency Operating Procedures (EOP);
   c. Safety Margin Assessment for Risk Informed licensing activities; and
   d. Assessment of PSA Success Criteria, including available times for operator actions.

II. Historic Perspective

II. Historic Perspective

II.1. Main Licensing Issues

The department of Modelling and Simulation at CSN (MOSI) is successor of several CSN groups, originated during the mid-80s, as a result of intense licensing activities in the review of Deterministic Safety Analysis (DSA, also known as Accident Analysis), and operating experience of Spanish Nuclear Power Plants, including the assessment of start-up tests in national PWR/BWR plants (see [7], [8], [9], [10]).

At the post-TMI times, Probabilistic Safety Analysis was already starting to be used in several licensing applications. The question of the consistency of deterministic and probabilistic studies was already posed in different licensing groups and reflected in the following issues:

- To which extent and at what stage of the PSA a significant change in stand-by safety systems initiation set-points, with obvious impact in DSA, could be reflected in the PSA results (issue 1).
- To which extent both DSA and PSA covered different operator behaviours, including for instance, time delays in the manual actions (issue 2).

II.2. Activities in the Development and Application of Simulation Tools

These questions were adopted as subjects of research within the "CSN Accident Analysis Research group", later enlarged into the "CSN Department of Developmental Programs", along with a thermo-hydraulic program at the national level (see [7]) which included:

- Intense participation in the validation of the USNRC RELAP-TRAC thermo-hydraulic codes trough the ICAP and CAMP programs.
- Development of CSN's own engineering simulators with capability for non-break transient simulation in national PWR/BWR plants. These developments were closely related with some previous activities related with start-up tests, and they are, at present, the TIZONA and TRETA replica codes (see [8], [9], [10]).
- Development of the BABIECA simulation driver, able to build customized computerized models in the form of topologies of simulation modules that the user can take from a library which includes, among others, those that replicate vendor design codes. BABIECA constituted the embryo of the present SCAIS platform (Simulation Code System for Integrated Safety Assessment) largely described in Section IV.

On the other hand, as a result of Spain joining the EU, CSN personnel had access to the Joint Research Centers (JRC), in particular to the incipient work made at JRC-Ispra on combining both deterministic and probabilistic safety analysis techniques. Realizing the potential of this pioneer work to answer the PSA consistency issues, CSN actively cooperated with this project, coupling the BABIECA simulation driver of TRETA with the original JRC-Ispra DYLAM code (see [11], [12], [13]). The resulting coupled code was applied to a scenario of steam generator tube rupture (SGTR)

in Jose Cabrera NPP. Included in this project was also the development of an HOI (Handbook of Operator Instructions) BABIECA module to simulate an operating crew that follows perfectly the available set of emergency operating procedures (EOPs) (see [7], [11], [14], [15], [16], [17], [18]).

1988-1991	1992-1997	1998-2004	2005-2008
TRETA-TIZONA	**TRETA/DYLAM/HOI**	**TRETA-MAAP-RELAP/ DENDROS/COPMA**	**SCAIS**
Transient Analyses software packages providing help to licensing work in the practical arena	Incorporation of Automatic delineation techniques and EOP simulation Application to (SGTR) EOP verification	Incorporation of a Modernized Scheduler, COPMA and MAAP Application to (SGTR) event tree delineation and EOP verification (multiple tube rupture)	Consolidation and modernization plan
Ref. [7], [8], [9], [10]	Ref. [7], [10], [11], [12], [15], [16], [17]	Ref. [7], [17], [18], [19], [20], [21], [22]	Ref. [23], [24], [25], [26]

Figure 1. SCAIS development: Historical perspective.

During the decade of 1990, CSN had also access to the results of the Halden Project COPMA-II system with capability to simulate procedures. This system was designed mainly as an operator support system in following operating procedures. However, it was also possible to simulate the procedure instruction effects on a plant simulator model coupled with COPMA-II. With the experience gained from the development of HOI, CSN-MOSI cooperated with the Halden Project in this version, being also actively involved in the development of the COPMA-III version that was coupled to BABIECA (see [7], [17], [18]). Again, this was the embryo of an in-house development better adapted to ISA needs, namely, the SIMPROC code currently linked to SCAIS (see Section IV).

Finally, during the last nineties and the first decade of the new century, the validated versions of the severe accident code MAAP and the thermal-hydraulic code RELAP-5 were also coupled to the system and a second generation scheduler, DENDROS (see Section IV), completely replaced the DYLAM driver for scheduling of events (see [7], [20], [21], [22]). Figure 1 summarizes chronologically the evolution.

All these developments afforded the most complex deterministic issues. In addition, on the probabilistic side we also implemented software to model and compute large event tree/fault

tree models of Spanish Plants (see [7], [27], [28]). This included not only assimilation and setup of existing external software but also alternate approaches like Binary Decision Diagrams, BDDs (see [29], [30], [31], [32], [33], [34], [35], [36]) for PSA level 1 and implementation of software modules for PSA level 2 Accident Progression computations (see [7]). They will be described in Volume II.

The resultant software package was the starting point of a process of consolidation and modernization to accommodate the product to modern software standards and tools, such as object oriented programming in C++ language, central data base and code connectivity (see [23], [24], [25], [26]). The process ended with the consolidation of the so-called SCAIS platform (Simulation Code System for Integrated Safety Assessment). Section IV describes it with special focus in its deterministic modules and features, leaving for Volume II the more advanced and recent developments in probabilistic components.

II.3. Progress in the Theoretical Developments

The code system composed by the coupling of TRETA, TIZONA, MAAP, RELAP, DENDROS, COPMA-HOI and BABIECA, resulting from the above described research programs, followed the so called Deterministic Dynamic Event Tree (DDET) approach, also used by other international groups (see [37], [38], [39]). In 1992, most of these groups participated in a meeting in Turkey (see [37]), organized by Prof. Tunc Aldemir, an advocate of the alternate Cell to Cell Mapping Technique (CCMT) approach, based on the reduction to a very large Markov system of the dynamic equations of physical systems where discrete events may occur with transition rates depending on process variables. At this meeting, Prof. Jacques Devoogth from Université Libre de Bruxelles (ULB) described his Theory of Probabilistic Dynamics (TPD). It was recognized there that this theory could provide a better theoretical framework, as it was able to cover the underlying concepts of both types (DDET and CCMT) of existing methods in a unified approach (see [37], [38], [39]).

TPD was initially more focused on the so called "living PSA", where the time evolution of the transition rates was at the slow aging scale. Working together with Prof. Devoogth himself, we could show, as expected, that the unfolding of event trees could also be addressed by the theory. Transition rates vary in this case in the accident time scale and, provided that they are conditioned only by automatic set-points, TPD could be efficiently applied. This clarified issue 1 discussed in Section II.1, although delays due to operator actions (issue 2 in same section) were not included. This was the reason to expand the theory to the more realistic cases where the transition rates were conditioned by other type of constraints, (alarm activations followed by stochastic delays, level 2 PSA stochastic phenomena) and/or by given system hardware configurations like those associated to failures (see [40]). The extension of the TPD to stimulated delays was baptized as Stimulus Driven Theory of Probabilistic Dynamics (SDTPD) (see [41], [42]) and completely clarified issue 2. Prof. Labeau, successor in ULB of Prof. Devoogth, contributed much to the extension.

SDTPD was a right answer to the issues that were posed. It was a general solution but at the same time it was difficult to implement in the engineering arena, where so much work was already done on event tree/fault tree (ET/FT) models for PSA and dynamic plant models for DSA.

From the ISA perspective, it is indeed a must that any new development should be implemented through interface links with the existing DSA/PSA tools, otherwise partial results of such a large risk assessment process cannot be checked. This was the objective of the development of the present Theory of Stimulated Dynamics (TSD, see [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53]) that, although rooted and inspired in SDTPD, thus able to afford the issues, was designed in such a way that it could provide those interfaces, therefore being fully compatible with current PSA models and techniques (FT and probabilistic quantification). TSD is the basis of the so called Integrated Safety Assessment method, SCAIS (Simulation Code System for Integrated Safety Assessment) being the present computational platform which implements ISA following the TSD concepts. Figure 2 summarizes chronologically the development of this TSD theoretical framework.

1992	1996	2005	2008
Deterministic Dynamic Event Tree **DDET**	**Theory of Probabilistic Dynamics** **TPD**	**Stimulus Driven Theory of Probabilistic Dynamics** **SDTPD**	**Theory of Stimulated Dynamics** **TSD**
Coupling DYLAM-TRETA Application to SGTR ET and EOP of CNJC DENDROS development	First collaboration with ULB (Université Libre de Bruxelles) to find coherence among TPD and classical ET/FT methods	Expansion of TPD to stimulated delays. Transition rates dependent of stochastic delays (operator actions and stochastic phenomena)	Search for compatibility with current PSA ET/FT models and tools Damage Domain maps as Risk Region Exceedance Frequency as Risk Measure
Ref. [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22]	Ref. [40]	Ref. [40], [41], [42], [43]	Ref. [43], [44], [45], [46], [47], [48], [49], [50], [51], [52], [53], [54]

Figure 2. Development of Theoretical Framework for Integrated Safety Assessment.

Finally, these elements were recently complemented with additional developments to incorporate the uncertainties in event timing and boundary conditions (TFT, Transmission Functions theory; see [54], [55] and Volume II) required for the assessment of success criteria in PSA level 1 and for the APET computation in its extension to PSA level 2.

II.4. International Activities and Research Programs

Figure 3 presents the schedule of several national and international activities and how they fit into the present SCAIS development and application research program; it shows as well the partners that have collaborated in each action. The current programs focus on efficient methods for TSD/TFT implementation (see [54], [55]), particularly research on the TSD and TFT itself, damage domain searching, incorporation of FT/ET techniques at the transient level and data post-processing.

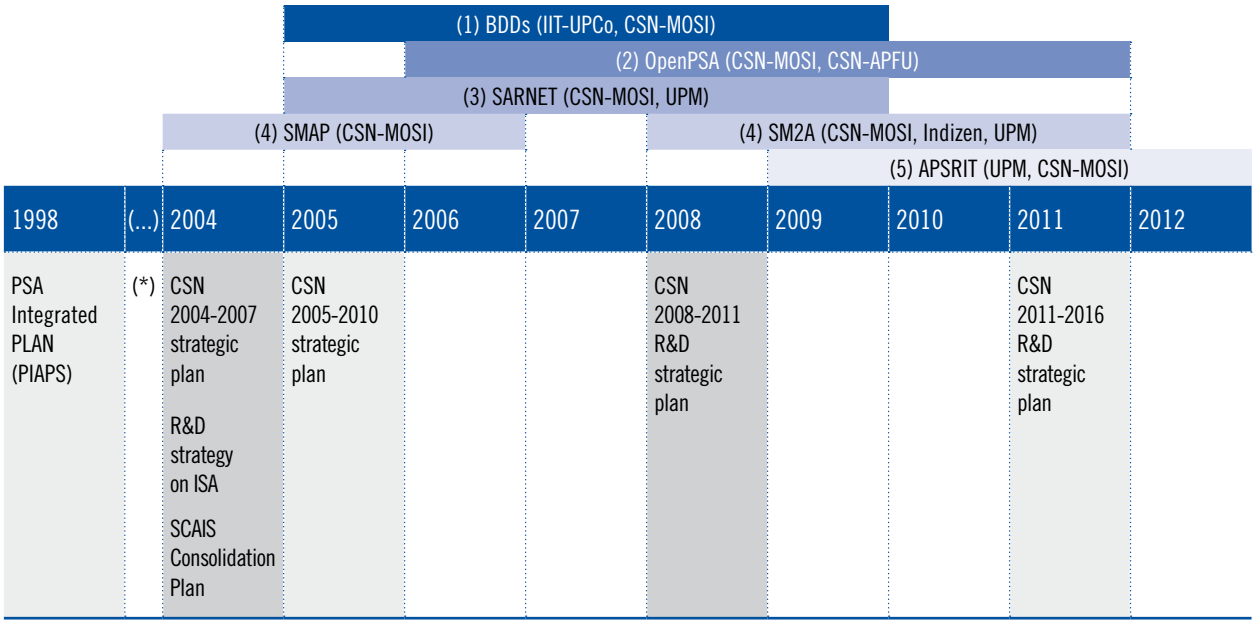

Figure 3. Schedule of natiional and international SCAIS related activities.

Concerning applications, we have participated in programs relative to incident analysis, safety margin assessment, technology neutral licensing methods and emergency procedures/ severe accident guidelines verification. It follows a brief description of the major projects:

- **Binary Decision Diagrams (BDDs).** This project (see [29], [30], [31], [32], [33], [34], [35], [36]) has provided the basis for using BDD representations of the FT´s that allow to incrementally performing Boolean products of FTs as they appear in the unfolding of the tree. Research continues to improve this important point, together with methods to modify the FT models at the transient level.
- **SARNET WP5.3.** Our participation in this international project was oriented towards the development of TSD as a unified approach for PSA levels 1 and 2 (see [43], [44], [45], [46], [47], [48], [49]). The main ideas and incipient methods were applied to a

small pilot project related with hydrogen stochastic deflagrations previously identified as relevant scenarios in some of the Spanish level 2 PSA. A containment module was also developed to be added to the BABIECA library.

- **SMAP-SM2A** (Safety Margin Assessment Application). Our participation in this international project (see [6], [56], [58], [59], [60]) aimed at consolidating major concepts like the frequency of exceedance as a measure of risk and the TSD capability to assess safety margins.

  Our participation in SM2A implied its application to different scenarios:

  - Loss of component cooling water (see [56], [58], [59], [60]).
  - Small Break and Medium break LOCA (see [60], [61], [62], [63]).

  The DENDROS-BABIECA-MAAP4 system was used for this purpose in order to check the PSA event tree delineation. The independent study included the identification of representative transients, damage domain searching and off-line estimation of exceedance frequencies.
- **APSRIT** (Advanced Probabilistic Methods for a Technology Neutral Regulation). This project is oriented towards the confirmation of the ISA-TSD method to verify risk in new technologies (see [64], [65], [66]). Research focuses on new aspects like increasing the scope of the damage domain search techniques. It involves applications to reactor protection system reliability in technologies that do not have the benefit of a long tradition in this field. The HTTR test facility, able to simultaneously produce both electric power and high temperature gas to feed hydrogen production facilities, was chosen as a pilot application.

The rest of this contribution will describe the progress during these years in order to be able to check each of the items involved in licensing safety cases of Spanish plants. It will provide main features and some details of the ISA-TSD-TFT approach integrated in the SCAIS platform, illustrated with some application results. This Volume I provides some of the details of the deterministic side, while Volume II will focus on the probabilistic side. Both territories and the overlapping areas will be distinguished in Sections III.2 and III.3 below.

III. Integrated Safety Assessment (ISA) versus PSA and DSA

III. Integrated Safety Assessment (ISA) versus PSA and DSA

The two traditional approaches to safety analysis in nuclear power plants are the so-called Deterministic Safety Analysis (DSA) and Probabilistic Safety Analysis (PSA). DSA has been and continues to be the main support for licensing design issues and Technical Specifications. However, there is an increasing trend to incorporate risk considerations, based on PSA, into different licensing activities. For example, although Technical Specifications have been traditionally derived from DSA, there are aspects like surveillance requirements or unavailability times that are better supported by PSA, when applicable. Moreover, some Technical Specifications have been recently developed on the basis of PSA.

In addition, regulatory bodies are increasingly using PSA for many other licensing activities. As an example, CSN makes intensive use of PSA for inspection planning, categorization of inspection findings, incident analysis as well as control of operational aspects (maintenance rule, human reliability and safety culture), among others.

It is therefore of capital importance to ensure that both DSA and PSA have internal and cross consistency; this is the aim of the development of the Integrated Safety Assessment (ISA) at CSN. Being an integrated methodology, ISA allows performing consistency checks involving deterministic and probabilistic aspects of both types of traditional methodologies. In the following we describe some of the ISA capabilities with special focus in the deterministic aspects. Probabilistic issues that can be checked with ISA will be addressed in Volume II.

III.1. Main Concepts

Some basic concepts that are commonly used in DSA and PSA are also at the basis of ISA. In addition, there are other concepts characteristic of ISA, some of them not really new but not explicitly used in DSA and PSA. A good assimilation of all these concepts is essential to understand the relationships between DSA and PSA and the ISA capabilities to assess internal and cross consistency of these approaches to safety analysis.

III.1.1 Safety barriers and safety limits

A basic safety strategy of Nuclear Power Plants is confinement by means of successive physical barriers. However, there are different degradation mechanisms or processes which could impair the integrity of those barriers. Identifying possible barrier failure mechanisms and preventing them is an objective of the plant safety design. Barrier integrity is characterized by structural integrity indicators and the possibility of barrier failures is associated to those indicators exceeding certain limits, usually referred to as *safety limits*. Without exceeding safety limits of a given barrier we may guarantee that releases of radio-nuclides through that barrier are kept to an acceptable minimum. Safety limits are hierarchical, i.e., there is a safety limit logic, meaning that higher level safety limits are proved to be not exceeded conditional to the state of certain logical combinations

of lower level safety limits. For instance, if the coolant keeps sufficient sub-cooling margin there is little point to worry about two phase degrading phenomena; if DNB limits are not exceeded, cladding burnout phenomena are precluded and if the cladding temperatures do not reach certain limits, cladding oxidation will be limited.

III.1.2 Safety functions and success criteria

A safety function is a set of automatic or manual actions aimed at preventing failure mechanisms in protective barriers or at minimizing the release of radioactive materials.

Depending on the context (DSA, PSA, emergency operating procedures...) safety functions can be defined with different level of detail although the total capabilities provided by the set of safety functions are always approximately the same. The following list is a possible catalogue of safety functions but it is given only as an illustrative example and cannot be taken as a consolidated list:

- Reactivity control and power generation
- Adequate core cooling
- Maintenance of reactor coolant inventory
- Heat extraction from reactor coolant (heat sink)
- Control of Reactor Coolant System pressure
- Containment isolation
- Control of containment pressure and temperature
- Control of combustible gases in containment

Safety functions are not independent of each other. Relationships include contribution of a safety function to another one (e.g., maintenance of coolant inventory contributes to adequate core cooling) and precedence of some safety functions considered of higher priority. These relationships provide, as in the case of safety limits, some logical structure to the set of safety functions.

In most cases, safety functions are performed by safety systems, automatic or manually initiated. A safety system can contribute to one or more safety functions and these contributions altogether can be referred to as the *system safety function*. Performance of the system safety function is characterized by suitable process variables. It is considered that the system safety function is successful if it provides an effective contribution to all the safety functions that the system is intended for. In practice, some thresholds in the characteristic process variables are defined to discriminate success from failure of the system safety function. Accordingly, those thresholds are referred to as success criteria of the system safety function. As a general rule, *success criteria* are system specific, valid for any scenario, although there are cases where they are modified for particular plant states or accident sequences.

An important feature of safety systems is that the success criteria of the system safety function may be converted into system configurations (i.e., number of available trains, alternative systems

available, …). This is done through a separate study showing that some configurations guarantee an adequate performance of the system safety function with sufficient reliability and availability.

Dealing with configurations is more convenient in a context of system reliability analysis and made system reliability techniques like Fault Tree-Event Tree (FT/ET) and the like to be progressively incorporated. This is why minimal configurations for fulfillment of system safety functions are also called system *success criteria*.

As in the case of safety limits, system safety functions are also logically related. Apart from logical dependencies between different safety systems there is also some logic aimed at implementing basic principles of redundancy, diversity, and so on. System safety function specifications include requirements about when they should be initiated. Again those will be defined in terms of limits that, when exceeded, call for the initiation of the system safety function. These initiation criteria are a particular case of stimuli (see Section III.1.4).

Safety functions try to avoid degrading phenomena or to trigger protective phenomena in such a way that the plant state is driven away from conditions challenging the protective barriers. Very often, safety systems do not act directly on the phenomena they try to avoid or promote but on other phenomena which are necessary (for phenomena to be avoided) or sufficient (for phenomena to be triggered), provided that they are easier or more convenient to handle, have less uncertainty or are better measured. As seen in the examples, the process variables involved in the different formulations may be very different. The regulations fix the required barrier safety limits and minimum criteria for the safety systems, but designers may also use more convenient ones, that we will call design safety limits or design safety system criteria.

The protective phenomena may also be induced intrinsically when the process variables enter certain regions, giving rise to the concept of intrinsic safety. For instance a certain geometry design may induce natural convection phenomena without any need of external actions via systems. A most classical example is, of course, the Doppler effect that induces negative reactivity.

III.1.3 Dynamic and Static Events

An event is an occurrence in a discrete time point. Relevant characteristics of events are, on the one side, when and why they occur and, on the other, what they consist of, i.e., what are their effects.

From the point of view of their occurrence, there are cases where events are deterministically linked to the fulfillment of some conditions while in others they occur in a random manner with possible probabilistic dependencies. This allows for qualifying events as deterministic or stochastic. Nevertheless, an event can always be considered as a probabilistic concept since a deterministic event can be seen as a particular case of random event with its probability given by a concentrated function (e.g., Dirac's delta function) of the conditioning variables.

From the point of view of their effects, there can be many different types of events. However, in the context of safety analysis of nuclear power plants, we are particularly interested in two types of events, namely, dynamic events resulting in dynamic transitions, i.e., sharp changes

in the trends of plant variables, and static events not doing so. In the following, some examples of dynamic and static events will be given.

When considering events as probabilistic objects, the set of possible event outcomes configures a probabilistic space. For events consisting on initiation of a safety function the event outcome can be defined in terms of success or failure of the safety function or in terms of successful or failed system configuration as explained above, resulting in different descriptions of the probabilistic space.

The importance of events in quantitative safety assessments is related to the efficiency of the safety measures taken. Note that dynamic events induce phenomena that change the time evolution of the process variables, preventing them (or not) from entering unsafe regions while some types of static events may condition the occurrence of dynamic events.

A dynamic transition may be caused by dynamic events such as the start-up of a stand-by system, the shutdown of a working system or by the occurrence of a stochastic phenomenon. A dynamic event can only occur if some conditions are met. A stand-by system (most often a safety system) can be initiated or a working system can be tripped either automatically when some set-point is reached or manually when operators are required to do so by some operating procedure[1]. Stochastic phenomena can only occur when some process and/or environmental variables are within specific intervals.

III.1.4 Stimuli and their activation

In general we call *stimulus* the set of conditions that make possible the occurrence of a dynamic event. Again, they usually adopt the format of exceeding process variable thresholds, although they may be combined with other features, like the state (e.g., availability) of plant systems. When the plant state matches the conditions that define a particular stimulus we say that this stimulus is activated.

The activation of a stimulus is a static event since it does not result by itself in a dynamic event. Moreover, in the general case, if the dynamic event occurs, it will be randomly delayed with respect to the activation of its stimulus. Only in the case of automatic actions, the stimulus activation and the dynamic event are practically simultaneous but, even in this case, they need to be distinguished. For example, reaching the set-point of an automatic safety system (stimulus activation) is conceptually different from the start-up of this system (dynamic event). As a result, static events are also crucial, especially when they refer to changes in the state of the activation of the stimuli, given the fact that activation is, by definition, a necessary condition to open the possibility of the dynamic event.

1. There are cases where a non-demanded initiation of a stand-by system or an unintended trip of a working system are considered as initiating events of an accident sequence but they are never assumed in the middle of a sequence initiated by another event.

III.1.5 Sequences of Transitions, Sequences of Events and Event Trees

The concept of sequence is very general and can be defined as an ordered set of events. However, depending on the types of events that define the sequence, we can consider different types of sequences. For example, we can talk about *sequences of [dynamic] transitions,* also called *dynamic sequences,* if we consider that two sequences are equal if they contain the same dynamic transitions (resulting from the same dynamic events) in the same order, no matter what static events they contain.

On the other hand, we may consider also static events, e.g., stimulus activation events, in the definition of the sequence. In this case we use the more general term *sequences of events.*

A sequence of any type is initiated by an event that induces a plant transient. From then on, different events may come into play, depending on the particular evolution of the plant dynamics and on the probabilistic properties of the events. All the sequences started from the same initiating event have a common stem and, as new events are being considered, the resulting sequences will have some common parts. This allows for a tree representation of the whole set of sequences where a branching point appears whenever the possibility of occurrence or not of a new event is considered. Such a tree is referred to as an *event tree*. It is clear that, depending on the type of sequences being used, there will be also different types of event trees.

The end of a sequence is defined by any of two conditions, namely, that one or more specified safety limits are exceeded or that a stable safe condition has been reached. However, in many cases, achieving a stable safe condition without exceeding any safety limit could take a long time. To avoid this difficulty, it is customary to define a mission time that, if reached, marks the end of the sequence. From the point of view of sequence characterization, reaching the mission time is considered equivalent to reaching a stable safe state.

No matter what type of sequence is being considered, a sequence cannot be assimilated to a particular time history of the evolution of plant variables. This means, among other things, that a sequence cannot be simulated as such. When simulating sequences, there are a number of uncertainties to be considered which include parameter uncertainty both in models and initial conditions, variability in occurrence times of events and uncertainty in boundary conditions of the simulations. From this point of view, a sequence can be viewed as a large group of possible transients, each one resulting from assigning specific values to the uncertain items involved in the sequence. In this document, transients within a sequence will also be denoted as *paths* because they may be associated with trajectories inside the sequence. Any path in a sequence can be simulated but none of them can be identified with the sequence as a whole.

As a result, the probabilistic space defined by the event outcomes can be enlarged with the sequence uncertainties, usually represented also by probabilistic models. This enlarged probabilistic space is the working field of ISA and the elements of this space are the plant transients (or paths) which are compatible with sequence restrictions. The ISA probabilistic space is a generalization of the probabilistic spaces of DSA and PSA which allows for the use of ISA as a tool to perform consistency checks on the traditional methodologies.

III.1.6 Sequence success criteria and failure domain

The objective of protective actions and safety functions implemented along the sequence is to avoid exceeding specified safety limits. As indicated earlier, there are two conditions, any one of which defines the end of a sequence. If the sequence terminates because some specified safety limit has been exceeded, it means that the implemented safety functions have failed or, at least, that they have not been effective enough. In this case it is said that it is a ***failed*** sequence.
On the contrary, if the sequence ends because a stable safe condition has been achieved or, alternatively, because the mission time has been reached, the sequence is qualified as ***successful.***
Therefore, the safety limits specified for a given sequence in a particular analysis discriminate successful from failed sequences and can be properly called ***sequence success criteria.*** It should be noted that *safety function success criteria* and *safety system success criteria*, as defined in III.1.2 above, are dependent on the selected *sequence success criteria* since not all the safety limits require the same level of performance of the different safety functions to avoid being exceeded.

Another point to take into account is that a sequence seldom can be qualified as successful or failed as a whole. When a sequence is considered as a group of possible transients, as discussed in Section III.1.5, it is clear that some of those transients may result in exceedance of the specified safety limits while others may not. In other words, the sequence end state *(failed/successful)* is an uncertain variable as a consequence of the uncertainties involved in the sequence.

Since each individual transient within a sequence results from assigning specific values to the involved uncertain items, the whole set of transients, i.e., the sequence, can be described also as a geometric space with as many dimensions as the number of uncertain items being considered. The coordinates of a particular point in the sequence space are a unique combination of values of the uncertain items and, therefore, a point in this space represents a particular transient belonging to the sequence. Additionally, each point can be marked as failed or successful depending on whether the transient that it represents results in safety limit exceedance or not. The set of failed points defines a region of the sequence space which is called the *sequence failure domain.* Note that the failure domain of a sequence is not necessarily a contiguous region. The concept of failure domain has been extensively used in the ISA approach as will be explained and illustrated later (see Section VI).

III.1.7 Transient envelopes

When the performance of safety systems or the adequacy of safety functions need to be ascertained for a large group of transients, the use of transient envelopes can be very efficient in reducing the number of cases to be analyzed. The underlying idea can be explained with an extremely simple example. Let us consider two transients, A and B, where some safety limit S is challenged. Let us also assume that, without actually analyzing them, it can be demonstrated that the level of challenge to S is higher in transient A than in transient B. Then, if the analysis of transient A reveals that S is not exceeded, it is not necessary to analyze transient B. This idea is often expressed by saying that transient A covers transient B from the point of view of safety limit S.

Unfortunately, this simple idea is not directly applicable to most practical cases where there are several safety limits to take into account and different types of phenomena that could challenge a given safety limit. But, fortunately, the idea can be extended to make it applicable to practical cases.

Let us consider a more or less large group of transients with some common properties. Let us also consider a set of safety limits that should not be exceeded in any transient of the group. And let us assume that each safety limit may get challenged because of different mechanisms or phenomena taking place during plant transients. Under these assumptions, we can try to select a reduced number of transients from the group such that:

- All the possible types of challenge to every safety limit are represented in this set of selected transients.
- If any safety limit is challenged through a particular mechanism in a transient of the large group there is at least a transient in the selected group where the same safety limit is challenged in a higher degree through the same mechanism.

Then, we say that the selected set is an *envelope* of the large set from the point of view of the safety limits being considered. An envelope will be properly defined if it is minimal, i.e., if no transient of the envelope can be removed without losing the enveloping character of the remaining set.

The value of envelopes is that they allow for analyzing the adequacy and efficiency of safety system actions only in the enveloping transients. If the result of this analysis is that no safety limit is exceeded in this reduced set, it can be ensured that those safety limits will not be exceeded either in the large set of transients under the envelope.

Looking for envelopes is not an easy task and requires very sophisticated techniques. Very often, it is difficult to find a set of enveloping transients from within the group to be enveloped. However, the enveloping transients should be understood as analysis cases rather than plant transients and do not need to be realistic. This way, an envelope can be configured using artificially distorted transients provided that they match the common characteristics of the group to be enveloped. A transient of the envelope can be obtained, for example, by taking a transient from the group and distorting it by changing assumptions, model parameters or boundary conditions in such a way that the challenge to one or more safety limits gets magnified.

It must be stressed that the very purpose of enveloping transients is to provide upper bounds for challenges to safety limits, not to represent the plant behavior.

III.2. DSA approach

As indicated before, DSA is still the main support for licensing issues related to plant design and Technical Specifications. The purpose of DSA is to verify that safety systems, as designed, are able to avoid exceedance of specified safety limits in those scenarios matching the assumptions that were taken as design basis for those systems and that the radiological consequences of such scenarios remain also under specified limits.

Consistent with this objective, DSA mainly focuses on the behavior of automatic safety systems, although in a few special cases some specific operator actions are also credited. Likewise, the analysis is concentrated on the plant behavior while frequencies and probabilities are only taken into account in a mostly qualitative manner.

The objective of plant protections and safety systems is to avoid barrier degradations and each safety limit is intended to prevent a particular barrier failure mechanism. Although exceeding a safety limit does not necessarily mean that its corresponding barrier failure mechanism will occur, taking both things as equivalent is the usual approach in DSA in order to introduce an additional safety margin while simplifying the analysis. Because of that, safety limits are used as acceptance criteria in DSA. Not exceeding any safety limit ensures that barrier integrity is maintained. Exceeding a safety limit means that barrier integrity is, at least, seriously challenged and it is considered unacceptable.

In DSA, plant transients and accidents matching the design basis assumptions (e.g., not containing multiple independent failures, initiated from anticipated plant conditions, etc.) are classified in a reduced number of groups, according to their severity and the type of protection they require. Frequencies of these classes are not usually quantified but should be estimated to ensure that class frequency and class severity are inversely related and comply with applicable regulations. In these regulations, ranging from legal requirements to technical standards, class frequencies are usually limited in qualitative terms such as expected number of events in a time period (e.g., in one year or in the plant lifetime), although some standards also define numerical frequency ranges. On the contrary, severity is strictly limited by specific safety limits that must be maintained for any transient/accident of the class and by radiological limits to the consequences of those transient/accidents.

Complying with the applicable safety limits in each class does not totally avoid barrier degradations. Except for the lowest severity class where no barrier degradation mechanism is allowed, compliance with the required safety limits is compatible with some level of barrier degradation due to failure mechanisms not related with the class specific safety limits. In addition, some previous degradation level is allowed as an initial condition for the analysis. Because of that, the barrier analysis aimed at verifying compliance with safety limits in each class must be followed by the analysis of radiological consequences aimed at verifying compliance with specified radiological limits and validity of the specified safety limits.

The DSA approach is a paradigmatic example of the use of envelopes. For each DSA class and for each analysis phase (barrier analysis or radiological consequences), a reduced set of transients/accidents is defined such that they configure an envelope as described in Section III.1.7 above. Each transient or accident belonging to the envelope is called a *Design Basis Transient* (DBT) or a *Design Basis Accident* (DBA). The envelope itself is usually referred to as the *Design Basis Envelope* (DBE). Being enveloping scenarios, DBT/A are in most cases non-realistic analysis cases exclusively intended to verify the effectiveness of plant protections.

Deterministic assumptions about system configurations and other analysis conditions are used which become compulsory operating restrictions *(Technical Specifications)* needed to make the plant operation consistent with the analysis. Safety systems are assumed in their minimal configuration compatible with adequate performance of the system safety function. Accordingly, these minimal configurations will be taken in Level 1 PSA as a starting point for analysis and determination of system success criteria.

III.3. PSA approach

PSA is an approach to risk analysis providing valuable support for an increasing number of licensing activities in NPP and Regulators. In current practice, PSA focuses on risk from accidents with severe core damage, defined in terms of exceedance of one or more of the safety limits of the most severe class of design basis accidents.

The final purpose of PSA is to evaluate radiological risks which should be limited by high level safety goals or health objectives. However, the whole analysis is performed in three analysis phases called PSA Levels. Level 1 PSA identifies accident scenarios leading to severe core damage, computes their frequency (usually called *Core Damage Frequency,* CDF) and provides interface conditions for the next Level. Level 2 deals with accident progression in order to quantify the amount and likelihood of radiological releases (also called *source terms*) to the environment. Other Level 2 results are the *Conditional Containment Failure Probability* and the so called *Large Early Release Frequency*. Finally, Level 3 starts from the Level 2 source terms for quantifying the final radiological risk. In this document we will discuss Level 1 and Level 2 only because Level 3 methodologies are not consolidated yet.

III.3.1 Level 1 PSA

Level 1 PSA is a well established analysis methodology aimed at identifying possible severe accident scenarios and quantifying their expected frequency. Specific variants of the methodology are applied for accident scenarios started from operation at nominal power, low power conditions, shutdown states or due to internal or external events such as fire or flooding. However, the common approach, as described in abundant literature grouped under the name of PSA guides, consists of the following three main analysis stages:

1. Delineate the possible *sequences of events* (SOE) initiated by one among a set of possible initiating events and followed by protective actions and failures of safety systems or operator actions. The stage defines the sequence success criteria in terms of safety limits assumed equivalent to transition to severe accident conditions.
2. Determine system success criteria and identify, for each SOE, the resulting sequence of successful/failed safety system configurations. System success criteria are determined in such a way that if the last event in the sequence represents the failure (success) of a safety system the whole sequence is considered failed (successful), i.e., the sequence success criteria are considered exceeded (not exceeded).
3. Compute, for each SOE, the frequency resulting from its safety system configurations, by using, for instance, FT/ET techniques.

The concept of stimulus is not explicitly used in conventional PSA. However, an adequate treatment of stimuli is essential for a proper delineation of PSA sequences. Including a non-stimulated header (i.e., a non-demanded safety function) in a sequence means accounting for the beneficial effect of a safety function which is not actually involved in the sequence. The failure branch under that header would be the one representing the real evolution of the sequence but its assigned probability would be much lower than the real one. The final effect is the underestimation of the exceedance frequencies being quantified in the PSA, which is not acceptable from the safety point of view.

On the contrary, if a stimulated header is not included in a sequence, the exceedance frequency becomes overestimated. Although it could be argued that this is not a safety problem by itself, overestimating some contribution to risk may have the side effect of masking other plant vulnerabilities having real significant contributions to risk.

Therefore, there should be a bi-univocal correspondence between event tree headers and activated stimuli. Whenever a sequence has a branching point under a header, the corresponding stimulus must be activated in that sequence and whenever a stimulus becomes activated in a sequence there must be a branching point in that sequence under the corresponding header. Usual practices in Level 1 PSA do not always guarantee this correspondence.

While determination and verification of system success criteria is of capital importance in Level 1 PSA, it is usually an almost hidden part of the methodology. Verifying system success criteria means verifying that successful safety system configurations actually result in successful sequences. However, once system success criteria are considered verified, most of the Level 1 PSA applications focus on quantification and, at most, on some sequence delineation details and system success criteria are very seldom reevaluated.

The problem of system success criteria verification in Level 1 PSA totally parallels the problem of protection verification in DSA. Verifying that design basis configurations of safety systems are adequate to avoid exceedance of the required safety limits in DSA is similar to verifying that safety systems in their success configuration are adequate to avoid exceedance of sequence success criteria.

Consistent with this parallelism, design basis configurations are used, when possible, as system success criteria in Level 1 PSA. Moreover, verification of these success criteria or determination of additional criteria, when necessary, is done on the basis of an extension of the DSA methodology and, therefore, using transient envelopes. It can be concluded that, despite the "probabilistic" attribute that PSA has in its name, there are strongly deterministic aspects involved in the methodology which in case of Level 1 concentrate on the determination and verification of system success criteria.

The introduction of operator actions to initiate safety functions in Level 1 PSA raises the question of how to deal with time in PSA. Operator actions imply random delays between stimulus activations and initiation of safety measures. It is evident that a delayed safety measure, at a certain delay value, becomes ineffective and must be considered failed. Otherwise, it is no point to keep it as a header of the event tree. This means that the maximum time elapsed since the measure is decided (stimulated) until it is executed should be part of its success criteria, so time is implicit in the concept. This is the important issue of available times that accompany manual actions and are a crucial consequence of the release of the zero delay assumption typical of automatic safety actions.

Another crucial consideration can be done about the need of paying more attention to time. The transition rates of the basic events of an ET/FT actually depend on process variables. For instance, the rate of failure of a valve depends on its temperature. But, even if these functional dependencies are not considered significant, the impact of stimuli is always present in the ET side. Indeed the transition rate associated with a header is zero unless its stimulus is activated. This implies a strong dependence on process variables related with stimuli and the time evolution of these variables should be known.

Finally, quantification of Level 1 PSA sequences is usually performed on the basis of Boolean models represented by fault trees. The issue of random delays is solved by introducing the concept of available time and considering that a safety action is successful when executed within the available time interval, using a successful system configuration or failed otherwise. This approach is efficient when only a random delay is present or when there are several independent, non-overlapping random delays. However, consideration of several delayed actions in a sequence is, in general, a difficult problem that cannot be solved by using only Boolean quantification schemes.

III.3.2 Level 2 PSA

The scope of Level 2 PSA is the progression of the severe accident sequences identified in Level 1. Safety systems that were already considered in Level 1 initially remain in their assumed configurations. If new safety systems come into play during accident progression, their configurations are incorporated as an extension of the ET/FT models of Level 1. No recovery is assumed for failed systems, except for failures resulting from the loss of support systems such as electric power supply, which are considered recoverable. In the case that an initially successful

safety system is repeatedly demanded during the accident progression, some failure probability is assumed due to the multiple demands. Other than that, no additional random failure is assumed in initially successful systems but consequential failures due to sequence events or extreme dynamic conditions should also be considered.

In the progression of the accident the concept of sequence success criterion is not applicable. The main purpose of Level 2 analysis is to determine source terms resulting from severe accidents and there is no acceptable limit for source terms. The only criterion is the smaller the better and the final results are given in the form of exceedance frequency curves (risk curves) of different release groups or categories.

The concept of success criteria of safety functions (or header success criteria) is not applicable either. One reason is that header success criteria are defined with reference to some sequence success criterion. In addition, the uncertainties involved in the level 2 analyses are much larger than in level 1 and any attempt to derive enveloping header acceptance criteria valid for a large number of sequences would lead to unpractical results. However, the boundary conditions that the occurrence of an event impose on the plant processes still have a strong influence on the consequences of the event and must be ascertained. The difference with respect to level 1 success criteria is that the verification must be done at sequence specific level, not for all the sequences where the header is present.

The Accident Progression Event Tree (APET) is a typical analysis tool for Level 2 PSA. It differs from Level 1 event trees in several aspects. One of the differences is that most headers of a Level 1 tree represent safety functions performed by automatic systems or by operators that follow well defined Emergency Operating Procedures (EOP). On the contrary, Level 2 headers (most often called nodes) of the APET represent stochastic phenomena or operator actions guided (rather than prescribed) by Severe Accident Management Guides (SAMG).

A consequence of this difference is that the outcomes of a Level 1 branching can be properly called success or failure because they refer to a safety function. However, the outcomes of a Level 2 node representing a stochastic phenomenon, usually resulting in unwanted effects, hardly can be qualified in terms of success/failure. In addition, SAMG actions, although intended to drive the plant evolution towards a safer state, may have significant undesired side effects and the global effect of the action may be highly dependent on the specific dynamic conditions at the time of the operator intervention.

Apart from the calculation of source terms, another possible result of Level 2 PSA is the Conditional Containment Failure Probability (CCFP). One could think that the conditions for containment failure can be seen as equivalent to a safety limit and that CCFP quantification could be similar to CDF quantification in Level 1. However, containment failure is not usually modelled as a deterministic process that occurs if and only if a given limit is exceeded. Instead, containment failure is modelled by probability distributions which are functions of stress variables. Consequently, even for CCFP calculation, the concept of sequence success criterion is not applicable.

III.4. ISA approach

As indicated, ISA tries to verify compliance with regulations and consistency in the design and safety assessments made by industry. Consistently with this intend, ISA is an integrated method where deterministic and probabilistic aspects of the safety problem are solved together, taking into account mutual dependencies.

The concept of sequence as an ordered set of events is also extensively used in ISA. In the general case, ISA makes use of *dynamic events* and *dynamic sequences* as defined in Sections III.1.3 and III.1.5 above. However, stimulus activations, being static events, are also explicitly taken into account. A dynamic sequence is identified only by the dynamic events it contains, i.e., two sequences of events containing the same dynamic events and differing only in stimulus activation events are the same dynamic sequence. It can be said that stimuli do not define the sequence but are a key point of the methodology.

Stimuli are accounted for in ISA in two main ways. First, all the dynamic events in a sequence must be stimulated; otherwise, the sequence is not physical and must be discarded. Second, transition rates associated to dynamic events are null while the corresponding stimuli are not activated and become non-null upon stimulus activation. Every activated stimulus must be taken into account in the probabilistic quantification. If the sequence contains the dynamic event associated to that stimulus, the transition rate and the time elapsed since the stimulus activation need to be taken into account. If the dynamic event is not present in the sequence but the stimulus is activated, the event transition rate and the time from activation to the end of the sequence are also necessary.

The ISA methodology strongly relies on simulation to determine the consequences of accident sequences. However, as discussed in Section III.1.5, a sequence cannot be assimilated to a particular time history. Treatment of sequence uncertainties and identification of failure domains are essential parts of ISA. If sequence success criteria are used, each simulated transient is evaluated against those criteria in order to find the failure domain. The concept of header success criteria is no longer needed since compliance with the sequence success criteria is a direct result of the simulation. This allows for using ISA as a powerful tool to verify the header success criteria used in Level 1 PSA.

The main basis of the ISA-TSD method (Integrated Safety Assessment based on the Theory of Stimulated Dynamics) is to lower the assessment from the system configuration sequence level, characteristic of Level 1 PSA, or from the envelope level, characteristic of DSA, to the transient level within each sequence by:

1) Considering sequences as large groups of transients accounting for all uncertainties compatible with the probability space under check, e.g., parameter uncertainty, initial conditions, variability in occurrence time of events and uncertainty in boundary conditions.

2) Simulating a number of those sequence transients in order to find the sequence failure domain, defined as the subset of sequence transients in the probability space ending in a failed state. The number of transients that need to be simulated depends on the desired accuracy of the failure domain characterization but, in general, this number is very high.
3) Providing TSD algorithms to compute the contribution to the exceedance frequency (of the safety limit used to define the failed state) of any transient belonging to the failure domain, then aggregating these contributions for all the transients there. Included as factors in those algorithms are the conditional probabilities of the safety system configurations characteristic of Level 1 PSA. Explicit consideration of stimuli ensures consistency of the set of safety measures included in every transient and allows for a proper classification of transients into dynamic sequences.

IV. SCAIS: Simulation Code System for Integrated Safety Assessment. The deterministic modules

IV. SCAIS: Simulation Code System for Integrated Safety Assessment. The deterministic modules

Leaving aside the theoretical aspects that inspire the detailed computational methods, ISA encompasses a lot of transient simulations and application of ISA then requires a set of simulation/computational tools. The computerized platform called SCAIS (which, as already mentioned, stands for "Simulation Code System for Integrated Safety Assessment"), has been developed for this main purpose. It is composed by a set of interconnected modules which, nevertheless, have their own entity and can be used as standalone tools or as modules of other methods as well.

Present days SCAIS (see [23], [24], [25], [54], [55], [60]) is the result of a consolidation and modernization program of a prior system. It is being developed in close collaboration with NFQ Solutions S.L. (previously Indizen Technologies S.L.), a software development company specialized in risk assessment. The Technical University of Madrid (UPM) also participates at the testing and application level. The objectives of this program do not only include improvements in technical capabilities but they will also facilitate an easier maintenance and future update. We limit the description to the transient simulation capabilities that are the heart of the deterministic analysis.

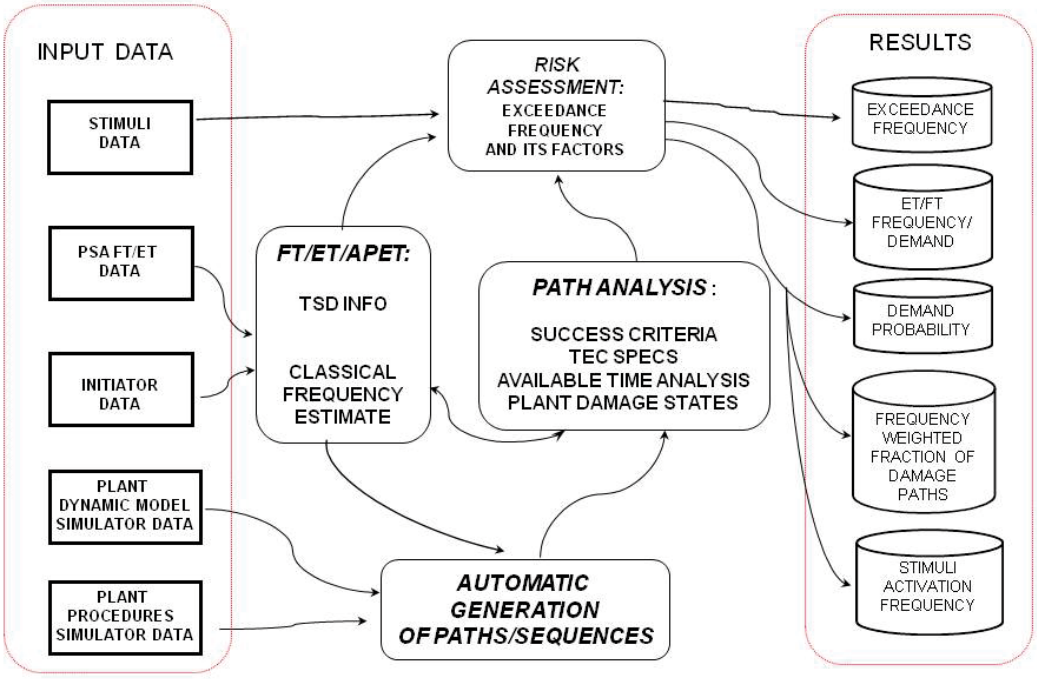

Figure 4. Simplified scheme of the ISA methodology and SCAIS conceptual blocks.

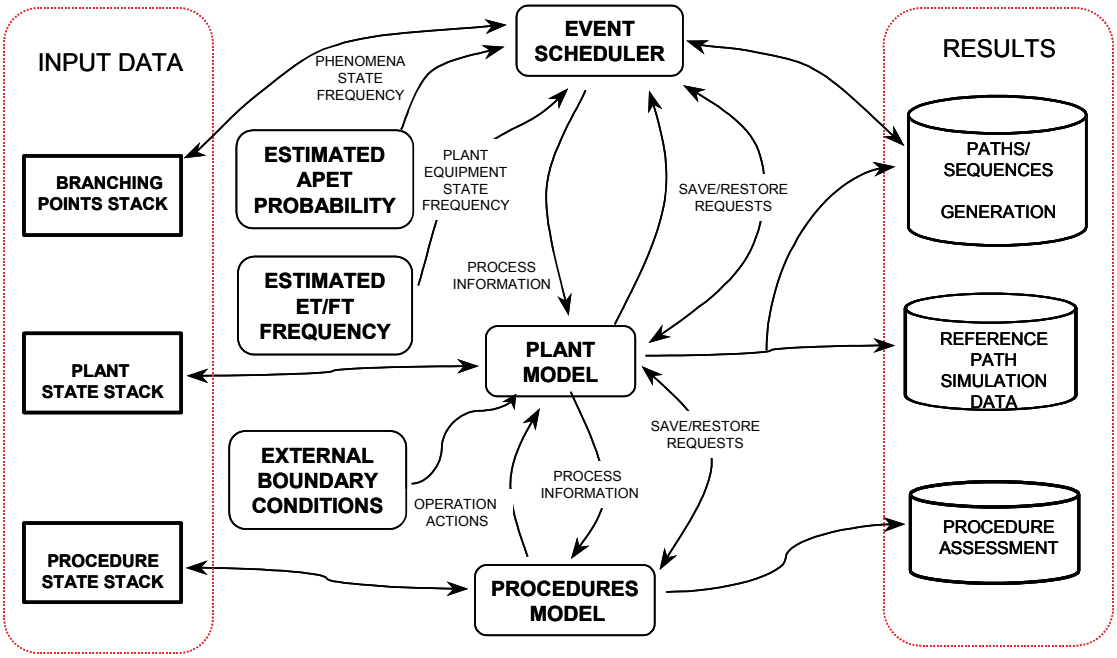

Figure 5. ISA/SCAIS elements for Automatic Generation of Paths and Sequences.

IV.1. Main Components of SCAIS for Deterministic Analysis

Among the different components of SCAIS, some implement deterministic aspects of the methodology while others are related with the probabilistic ones. Figure 4 presents a simplified scheme of the ISA methodology whose blocks parallel the main components of SCAIS, and Figure 5 details the structure of the lower block "Automatic Generation of Path/Sequences" of Figure 4. In the following description the main deterministic modules and their capabilities will be described with more detail, leaving for Volume II a deeper description of some of the more advanced deterministic as well as all of the probabilistic components. However, being SCAIS a tool for integrated analysis, references to the probabilistic modules is inevitable and will be included here to the extent needed.

Main elements of SCAIS are:

[1] BABIECA is the general simulation driver. It combines internal and external simulation modules from which the user can configure the plant model in the form of a topology of interconnected modules. Output information from a module (calculated results) may be used as an input for any other module that could need it. Each module may use its own solution algorithms with the only restriction to synchronize with the other modules at specified time intervals. BABIECA takes care of the overall solution by controlling the transmission of information among modules, solving feedback loops

if they exist and advancing the time step. These features provide a great flexibility to build powerful plant simulation models.

[2] DENDROS is the EVENT SCHEDULER that drives the dynamic generation and management of the different event sequences resulting from a given initiating event (see Figure 6). A branching point in a sequence appears whenever there are conditions for the occurrence of an event but there are chances for the event to occur or not or to result in different outcomes. DENDROS is able to identify and manage branching points and to ask BABIECA to open new simulation processes, one for each possible outcome of the event including lack of occurrence. The result is a dynamically generated event tree. DENDROS has been designed to guarantee modularity of the overall system and parallelization of the *dynamic event tree* (DET) generation.

[3] PLANT MODELS. As indicated above, a plant model is a particular user-defined combination of BABIECA modules able to simulate nuclear accident sequences.

The variety of plant models that can be configured ranges from using well accepted and validated external codes such as TRACE or MAAP to using only internal BABIECA modules. The possibilities that BABIECA offers to build plant models from its internal or external modules is discussed further below.

[4] SIMPROC is the simulator of operating procedures which interacts with BABIECA to implement the operator actions requested by the procedures. It is a special case of BABIECA external module because of the particularities of the interaction between plant and procedures. A more detailed description of the coupling between BABIECA and SIMPROC is described later and illustrated in Figure 7.

The [1] to [4] components of SCAIS implement the main dynamic modules as required by DET, including also those allowing for the verification of procedures via automatic pilot simulations.

[5] The PROBABILITY CALCULATOR (ET/FT/APET block in Fig. 4) is actually a collection of methods and algorithms that provide probabilistic quantifications. It may be optionally called to make estimates of the respective probabilities of the output branches of a branching point and to use them for elimination of some of these branches on the basis of low probability termination criteria. However, its major role is the computation of exceedance frequencies in coordination with the RISK ASSESSMENT module. This will be described in Volume II.

[6] PATH ANALYSIS MODULE, which performs the detailed analysis of individual event tree sequences through the simulation of specific transients (paths) belonging to the analyzed sequence.

In coordination with DENDROS, the PATH ANALYSIS MODULE defines multiple simulation cases, i.e., paths of the sequence, by varying values of uncertain parameters and/or time delays (human actions or stochastic phenomena). The aim

is to identify the Failure Domain (or Damage Domain) of the sequence with respect to the analyzed safety variable/limit pair. All the simulation results are stored in the SCAIS DATA BASE and made available to the RISK ASSESSMENT MODULE and the PROBABILITY CALCULATOR.

[7] The SCAIS DATA BASE is a SQL relational data base (POSTGRES SQL) used as a repository for input and output information. It stores all the input data and analysis results allowing for easily handling, analyzing and post-processing the huge amount of information generated during the analysis. The information stored in the data base can be accessed off-line making it possible to perform new analyses on the existing data without repeating the whole analysis and the simulations.

All main components of SCAIS, including the simulator driver BABIECA and the event scheduler DENDROS, are designed with object oriented architecture and implemented in C++ language. The whole SCAIS has been developed using open source standards (Linux, XercesC, libpq++) trying to make it platform independent.

Automatic generation of dynamic event trees is only possible with an adequate coordination between BABIECA and DENDROS and, sometimes, also coordinated with the PROBABILITY CALCULATOR. Figure 6 illustrates the branching procedure implemented in SCAIS.

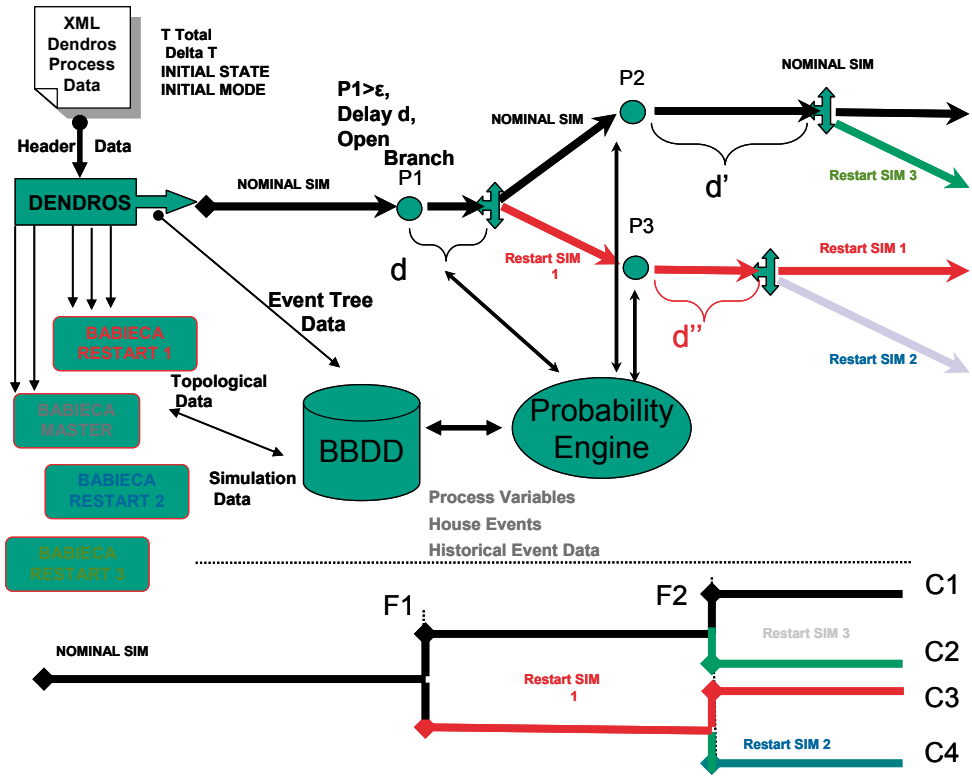

Figure 6. Overall BABIECA-DENDROS-Probability calculator coordination.

Branching criteria are represented by P_i (P_1, P_2, etc) in this figure. They define the conditions under which the stimulus of a dynamic event becomes activated and the branching consists of simulating both the occurrence and the non-occurrence of the event. When DENDROS detects that a branching criterion has been reached it initiates the branching procedure, possibly delayed by a time d if so specified in the branching rules. First, DENDROS asks BABIECA to generate a restart file with the current status of the simulation and the existing simulation process continues with the "nominal" option (occurrence or non-occurrence of the event, depending on the defined branching rules). Second, DENDROS spawns a new simulation process, i.e., another instance of BABIECA, initializing the simulation model with the stored restart file and forcing the "alternative" option of the branching point. This procedure is recursively continued until every simulation process meets some predefined termination criterion.

The upper part of Figure 6 represents the opening of new simulation processes while the lower part represents the corresponding DET resulting from this procedure.

IV.2. BABIECA Simulation Models. Internal and External Modules

A key feature of SCAIS is the capability to build simulation models for BABIECA from a catalogue of available simulation modules. Some of these modules can be taken from an internal library but BABIECA incorporates also the possibility to use independent external codes as simulation modules.

Internal BABIECA modules can be of very different nature. Some of them are very simple and frequently used computational algorithms, while others can implement some balance equations or a complete model of some plant component such as a heat exchanger, a pressurizer or a pump. In particular, the internal module catalogue includes all the modules that resulted from the development of the in-house replica codes (see [8], [9], [10]) TRETA (for PWR) and TIZONA (for BWR) which, in this way, become also part of SCAIS. The module library is not conceived as a terminated product since it can be permanently enlarged with new modules.

The use of an external code as a BABIECA module is achieved by incorporating some interface functions into the external code and by developing a specific wrapper, which is seen from BABIECA as a regular internal module, able to communicate with those interface functions through a message passing protocol, namely PVM. The difficulty to adapt the external code depends on its internal structure but for well structured codes following the basic programming standards the task can be afforded with very reasonable effort. It should be noted that the changes in the external code do not affect the physical model or the solution algorithm. Typical thermalhydraulic or severe accident codes such as RELAP5, TRACE, CATHARE, MELCOR, MAAP or ASTEC can be adapted to work as external modules for BABIECA. Specific wrappers have been already developed for MAAP (see [60]), RELAP5 and TRACE (see [25]).

A particular case of external code connected to BABIECA is the procedure simulator SIMPROC (see [24]). Although the connection philosophy is very similar, SIMPROC is not seen

as an additional module because, due to the particular nature of the operating procedures, it is connected directly to the driver of BABIECA.

Figure 7 illustrates the BABIECA-SIMPROC architecture. Internal and external modules can be combined in a simulation model and the whole model can be connected to SIMPROC through a specialized interface. BABIECA DB is the data base where the simulation inputs and outputs are stored, being a part of the general SCAIS data base. SIMPROC has its own data base, independent from the SCAIS data base.

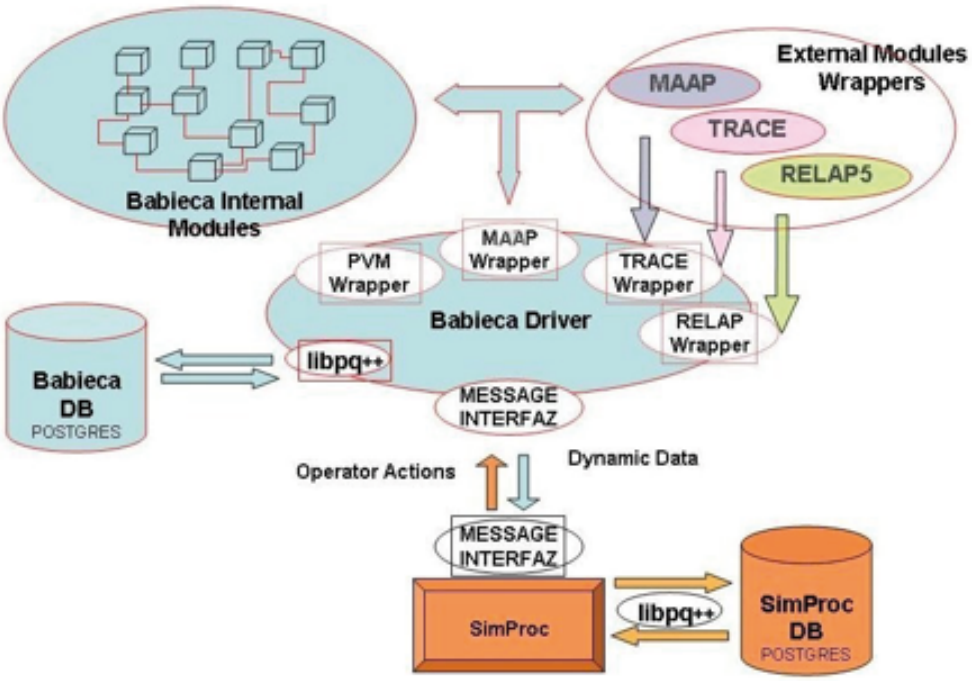

Figure 7. SIMPROC-BABIECA Architecture.

IV.3. Coupling Schemes in BABIECA

Building a simulation model in BABIECA requires to couple different simulation modules in a coordinated way. However, depending on how these modules relate to each other, they can be coupled in two different ways. When modules work together and exchange information at every time step it is said that they are coupled by boundary conditions. When a set of modules (including the case of a single module) is replaced by a different set at an intermediate time of the simulation, they are coupled by initial conditions (see [25]). These concepts are further developed below.

IV.3.1 Coupling by Boundary Conditions

Most often, coupling simulation modules to build a simulation model consist of specifying what module outputs are connected as inputs to other modules. The result is a network of interconnected modules that, in BABIECA terminology, is called a *topology* and may include both internal and external modules. The results of the simulation are given by the module outputs.

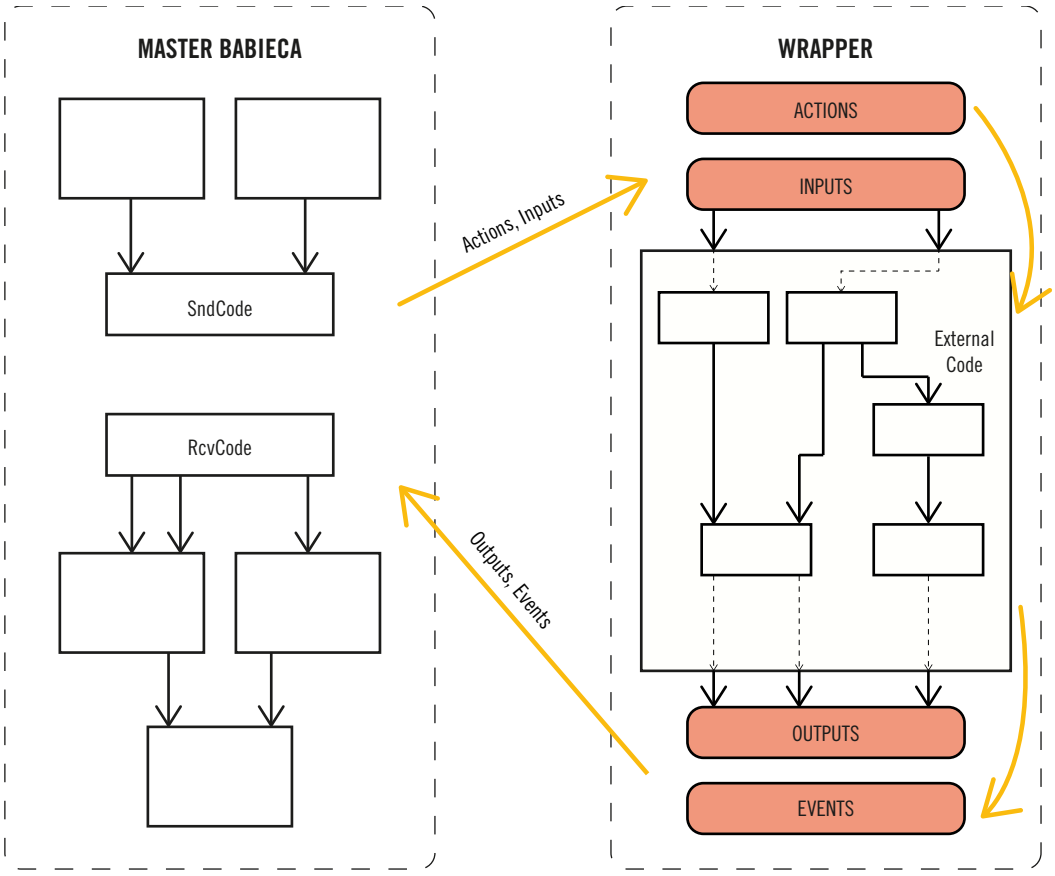

Figure 8: Use of the boundary conditions scheme to connect an external code to BABIECA.

In this type of connection, the outputs of any module act as boundary conditions for the other modules. The information is shared and exchanged at every time step during the simulation, so that the results of any module are conditioned by the results of the other modules in the topology. This type of connection is called coupling by boundary conditions.

The connection of an external code to BABIECA using the *boundary conditions coupling* scheme is illustrated in Figure 8. The outputs of BABIECA modules that must be sent to the external code are gathered by a special module called SndCode which communicates with the external code

wrapper. The wrapper translates process variables and action requests to the external code format before sending them to the actual code. Using this input information the external code advances its solution algorithm to the next synchronization point. The results, which can include process variables and identified events, are sent to the wrapper which sends them to BABIECA after the corresponding format translation. The information is received by the special module RcvCode which makes it available to any other module in the BABIECA topology.

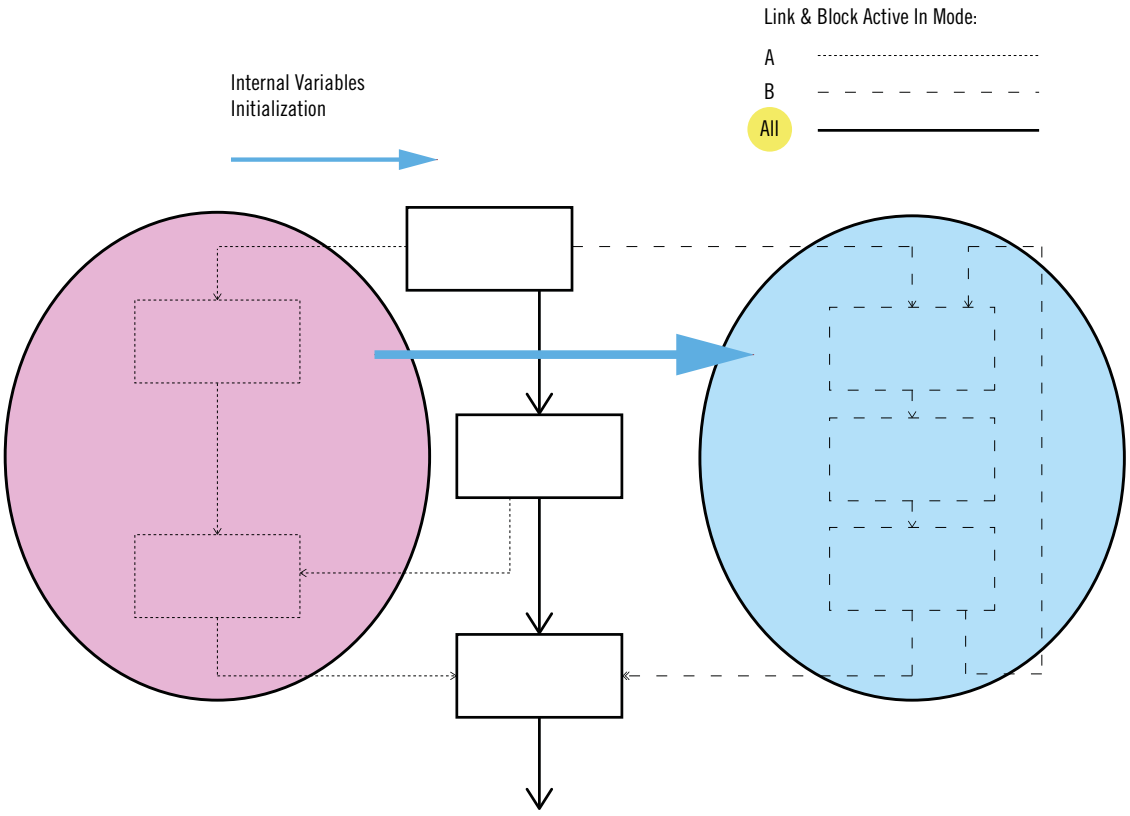

Figure 9: Use of the initial conditions scheme to replace a section of the simulation model.

IV.3.2 Coupling by Initial Conditions

There are cases where the evolution of the plant state during the simulation makes some module, or group of modules, to reach their modeling validity limits. In such case, BABIECA allows for the replacement of the invalidated modules by others able to continue the simulation. When this occurs, the last calculated conditions of the old modules are used to initialize the new modules, so that the simulation can smoothly continue. This type of connection is called *coupling by initial*

conditions. Just to mention a simple application example, coupling by initial conditions would allow for using a very fast homogeneous model while a fluid system remains subcooled and switching to a more adequate multi-phase model as soon as the system reaches saturation.

BABIECA implements the *initial conditions* coupling scheme by defining simulation modes and specifying which modules (internal or external) are active in each simulation mode.

The coupling by initial conditions scheme is illustrated in Figure 9. Modules and connections drawn with solid lines are active in any simulation mode. Dotted lines identify modules and connections that are only active in simulation mode A (left side of the figure) while dashed lines indicate that the corresponding modules and connections work only in mode B (right side of the figure).

Switching from mode A to mode B occurs when user defined conditions are met. At that time, the internal variables of A-mode modules are transferred to the B-mode modules which use them to initialize their own internal variables.

Any type of module, internal or external, can be coupled by initial conditions. However, those modules able to take the task in the middle of a transient must incorporate the corresponding initialization algorithms.

V. Application of ISA to Licensing. Deterministic Aspects

V. Application of ISA to Licensing. Deterministic Aspects

V.1. Types of Analyses

As indicated in Figure 10 below, a number of CSN licensing activities may be analyzed. They are classified in terms of whether the probabilistic side or the deterministic side is directly involved. But to ensure that all those analyses are consistent, it is essential to verify key interface topics that will be discussed here (Volume I) and expanded in Volume II.

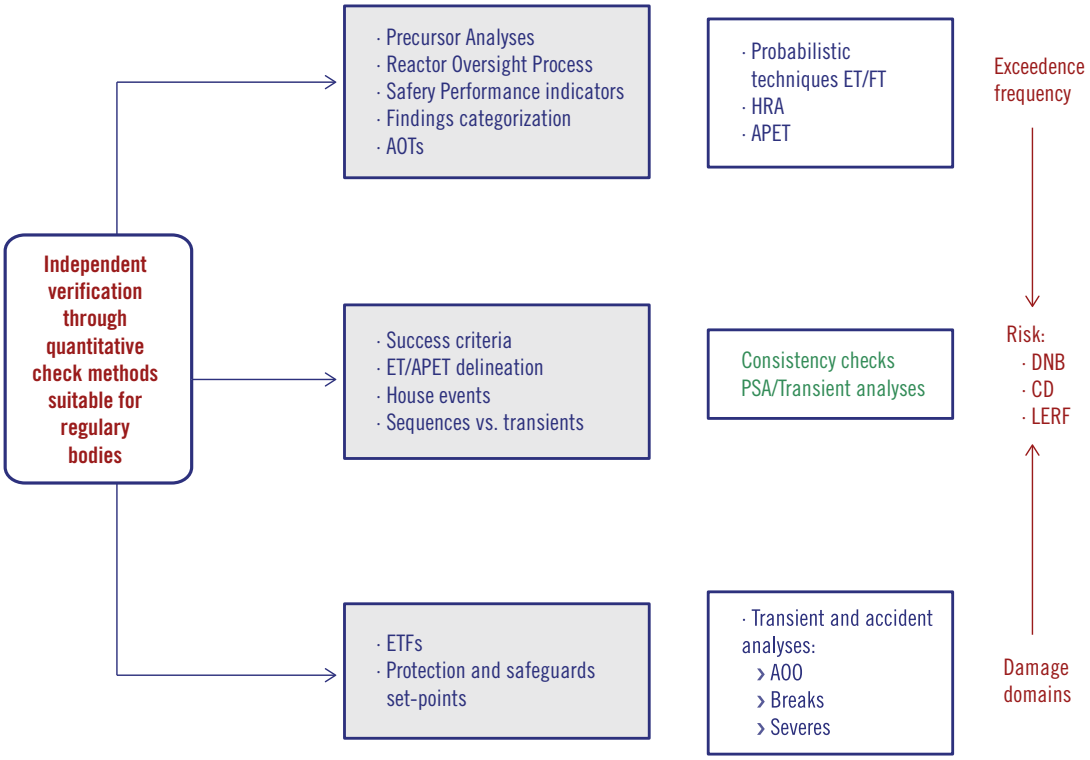

Figure 10. PSA and DSA methods and typical licensing applications.

V.2. Checking issues in DSA

As shown in Section III, in order to account for uncertainties while simulating a reasonable number of scenarios, the industry design approach verifies barrier integrity success, for each safety limit (as described in the safety analysis reports), in a set of so called Design Basis Transients (DBT)[2].

2. Also the term Design Basis Accident (DBA) is often used for referring to high severity DBTs. In this document we are using the term DBT as inclusive of any kind of design basis analysis scenario.

We recall that these are non-realistic scenarios distorted in both models and assumptions that are supposed to altogether cover all situations potentially challenging those safety limits.

One of the main reasons to use the DBT approach is its efficiency for the purpose of designing safety systems and their actuation criteria (set-point design) and the main purpose of the DBT analysis is to verify that the resulting set-points and safety system capabilities actually provide an adequate coverage for design basis compliant situations (also called the DSA transient space), i.e., they maintain barrier safety limits to the extent required.

However, the validity of this approach needs to be verified by checking that, for the existing set of safety systems and features, the set of analyzed DBTs actually configures an envelope of all the situations intended to be covered. Such an envelope is often referred to as the *Design Basis Envelope* (DBE).

Since different safety limits apply for different ranges of frequencies, the DBT is specific for each design class and the umbrella verification should also be checked for each of those classes. This is a difficult issue, traditionally ignored in licensing evaluations, which can be seen as a part of the verification of DSA.

Focusing on the deterministic verification of design envelopes, one should identify all the sequences of transitions that may occur under the envelope and account for all the uncertainties discussed in Section III.1.5 that characterize its transient space. Identification of sequences is not an easy task in a DBT environment because no indication is given in a DBT as to whether it belongs to a sequence or another, since this requires ensuring the sequence stimulus activations, as explained before.

For the purpose of verifying the DBE, it is useful to consider the transient DSA space as a probabilistic space and to consider ISA-DSA sequences composed not only by dynamic events but also by stimulus activation events. The ISA-DSA event trees identified in the process of DBE verification will be referred for short as DSA event trees. Let us recall that an activated stimulus, by itself, does not result in any change of the sequence dynamics but it results into a sequence header which means that the associated dynamic transition may occur or fail, giving rise to a branching point under that header. This way, occurrence of a dynamic transition requires the existence of its header in the sequence but non-occurrence of the transition could be either the result of lack of stimulus or actual failure of the header. These two situations need to be carefully distinguished.

Indeed, if a header stimulus is not activated in a given transient, the corresponding header protective action is not taken, so that the transient consequence is the same as if the header stimulus would be activated but the protective action would fail. This means that such a transient could belong to two different sequences of the same tree, namely, the one without that header and the one with that header failed. Due to the required high reliability of safety systems, the former has a much larger contribution to the frequency than the latter and, in addition, some failures of activated protective actions are considered as non compliant with the design basis assumptions.

Discrimination of these two situations is then an important point in the sequence delineation. Therefore, it is a must to verify the stimulus activation, showing the strong dependence of the sequence delineation on the stimulus design (issues 1 and 2 in Section II.1).

As a result of the design process, minimal safety system capabilities which are needed to guarantee the sufficiency of the header success criteria are defined for each DSA event tree header, sometimes specific for particular types of sequences. Minimal configurations of safety systems, able to comply with the system success criteria, and compliant with typical deterministic criteria such as the single failure criterion, are then assumed available in the context of design basis analyses. From the above discussion it can be concluded that not all the transients represented by DSA event tree sequences are compliant with the design basis assumptions. Only those transients belonging to sequences where all the activated stimuli are followed by the associated protective action, taken on time (i.e., within the available time window), are assumed to be covered by the design basis envelope.

The ISA method defines, identifies and computes *sequence Failure Domains* associated with *a safety limit,* as the set of sequence transients where that safety limit is exceeded. The steps that should be followed for DBE verification are the following:

1. **Identify the initiating events** that can result in design basis compliant scenarios. These initiating events should include, at least, all the event types assumed as initiators of the enveloping DBTs. However, it must be taken into account that part of the distortion of a DBT could be the use of unrealistic initiators not directly usable for the verification process. Uncertainties in initiating event parameters and initial conditions must be included in step 3 below.
2. **Develop the DSA event tree** for each identified initiating event. Minimal configurations of safety systems compatible with predefined success criteria should be considered in success branches of every branching point in the tree. Identify design basis compliant sequences, i.e., those sequences where every activated stimulus is followed by the corresponding protective action.
3. By performing the analysis of all the relevant uncertainties, **determine the failure domains** of design basis compliant sequences with respect to each applicable safety limit. The uncertainty analysis should also include those uncertainties related with safety systems in their minimal configuration in order to verify that those minimal configurations result in a system performance compatible with the assumed success criteria.

The validity of the DBE can be checked by analyzing the resulting failure domains. In a conservative licensing approach, the acceptance of DSA requires verifying success in all the DBTs. In this case, a non-empty failure domain in a design basis compliant sequence is a clear indication that there are situations matching the design basis assumptions that escape the assumed DBE.

In the case of a Best Estimate plus Uncertainty (BEPU) licensing approach, some level of safety limit exceedance is allowed in DBTs. This means that failure domains of design basis

compliant sequences are not necessarily empty. When this occurs, the conditional probability of the failure domain (given the occurrence of the sequence) must be evaluated and it should be lower than the exceedance probability allowed by the tolerance limits applied in the DSA. The probabilistic space in this case is only considering parameter uncertainty so even if this check requires a probabilistic quantification, it will be considered as a part of the deterministic verification of the DBE in the same way that the uncertainty analysis in DSA, when performed, is considered as a part of the DSA itself.

Other checks can be performed using all the sequences of the DSA event trees, not only the design basis compliant ones, mainly oriented to assess the sufficiency of the implemented safety functions and/or the need to enlarge the design basis. However, they are based on probabilistic quantifications and should be considered as a part of the probabilistic verification of DSA which is not discussed here.

V.3. Checking Deterministic Issues in Level 1 PSA

It was already stated in Section III.3.1 that there are important deterministic aspects involved in the PSA methodology. In particular, determination and verification of success criteria for safety systems and functions in Level 1 PSA is an extension of the DSA. This extension starts from an enlargement of the DSA probabilistic space, as defined in Section V.2, to include delays between stimuli activations and actual execution of their associated safety measures, which imply a variety of out of design situations. Among them, the enlargement (see Section III.1.6) implies that the system success criteria are no longer defined only in terms of minimal configurations but they should be accompanied by an available time whenever the possibility of manual initiation is considered.

Another extension of the probabilistic space consists of considering the possibility of using non safety-graded systems to perform safety functions. This implies first to consider all possibilities to barrier failure accounting for out of design safety system configurations compatible with the possible delays.

Of the three main stages of a Level 1 PSA, namely, sequence delineation, success criteria determination and quantification, the first two are essentially deterministic but unavoidable to develop the third stage where probabilistic methods and tools are mainly involved. Those will be briefly discussed.

V.3.1. Checking sequence delineation in Level 1 PSA

The stimulus activation problem already discussed in the context of DSA verification is also present in Level 1 PSA sequences. There should be a bi-univocal correspondence between event tree headers and activated stimuli as discussed in Section III.3.1.

It is, therefore, of primary importance to verify that the event tree sequences in the PSA study have been correctly delineated. However, this verification cannot be done without taking all the uncertainties into account. If a sequence header is not found stimulated for any combination

of uncertain item values, the header must be deleted from the sequence. The opposite occurs if a non-existing header is found always stimulated in the uncertainty analysis. The most difficult problem appears if the uncertainty analysis reveals that some stimulus is activated or not depending on the particular values assigned to uncertain items. In this case, the sequence should be split in two different sequences, with and without that header. This is not a special problem in the ISA methodology but adapting the classical PSA model to adequately represent this case could be far from trivial.

V.3.2 Verifying system success criteria in Level 1 PSA

As a result of the enveloping approach used to derive system success criteria (see Section III.3.1), typically, they are determined in such a way that they are valid for the highest possible number of sequences. Often, they are valid for any sequence in the Level 1 PSA study and in many cases, they are coincident with DSA system configurations.

However, in the enlarged transient space of Level 1 PSA, some of them may change if there are significant changes in the analysis assumptions or in the plant design. This occurs, for example when allowing for delays between stimulus activations and safety action execution, which amounts to new time dimensions in the ISA failure domains.

Because the automatic design space is the particular case of zero time delays, the system success criteria other than the available times remain in many cases the same as in the automatic design. However, at least a new extension of the failure domain searching analysis will be needed to account for these new dimensions that will provide a multidimensional available time domain as a function of the actuation times.

The procedure for verification of success criteria using ISA methods is then to verify that the safety functions performed by safety systems in their assumed success configuration and acting within the available time window are enough to avoid exceedance of the sequence success criteria. Success criteria get verified if all the sequences ending with a successful header have an empty failure domain. Of course, all the successful headers in the sequence, not only the last one, are assumed in their minimal success configuration. During the failure domain searching all the actuation times must be varied within the limits imposed by the proposed available times without discarding any combination a priori.

Another check that can be performed is that at no moment the dynamic performance of a safety system is under the safety function success criterion, i.e., under the minimal required performance as established by the design. This is of particular interest when executing operating procedures in some specified sequences, which allows checking for the adequacy of those procedures which, in many cases, are a result of the extension of DSA to the Level 1 scope.

Some additional peculiarities are also to be mentioned:

- Initiating events in PSA event trees are usually more realistic than their counterparts in DSA. This allows for an easier determination of the initiating events to be analyzed and their associated uncertainties.

- If PSA sequences are already delineated but they do not include explicit verification of stimulus activations, verification of header success criteria requires a prior ISA verification of sequence delineation as discussed above. Explicit discrimination of transients where a given header has not been stimulated from others where the header has been stimulated but has failed is a need for success criteria verification.

The special complexity of the available time issue requires some additional discussion.

The ISA failure domain accounting for time delays will in general show a complex shape as exemplified for instance in some cases of Section VI below. The simplest result could be found in case where these failure domains would be rectangular (parallelepiped shaped for more than two dimensions), which implies that the available time of an action is independent on the rest. In this case an available time is added to the existing minimal configurations to get the extension of the system success criteria.

For complex failure domains resulting from time delays there are cases where a bounding rectangular (parallelepipedic) domain can be found. The condition is that the simplified domain totally includes the real domain without crossing its boundary at any point. Assuming that any path (transient) inside the bounding domain is a failed path maximizes the calculated exceedance frequency but, if the results are still within the range of acceptable values, this practice can be acceptable. However, for cases where this solution is not practical, it is also possible to combine some independent available times with others depending on the specific occurrence time of other events.

V.3.3. Verifying Emergency Operating Procedures

When verification of an Emergency Operating Procedure (EOP) for scenarios in the Level 1 PSA space is the issue, simulations are run with an automatic pilot version of the procedures, as realistic as possible, by using our procedure simulator SIMPROC ([24], see Section IV) coupled to the automatic event tree SCAIS simulator ([23]). Timing to take the actions is predetermined using info from best practices and as operator crew task action studies indicate. The objectives of the procedure should be met and success relative to any of the safety limits should be assured. If this is not the case, the procedure is questioned at specific points.

VI. Examples

VI. Examples

As the preceding Sections have indicated, there are many deterministic licensing aspects that may be checked with ISA/SCAIS and/or its predecessors, the platform development covering historically different capabilities. In the References we list a sample of applications that have been performed, either as pilot projects to verify the system at specific points in time, or as specific plant studies. It should be clear however that referenced applications are those linked to developments, improving the system capabilities when new problems appeared. Other applications developed on a routine basis in support of daily licensing actions are not listed.

Some of these applications are more detailed below, in order to illustrate the type of insights, results and conclusions that can be obtained. They are complemented by several contributions presented in different meetings by partners in this developments (UPM and NFQ), which also provide a more detailed account of today's SCAIS capabilities (see [23], [24], [25], [26], [52], [53], [58], [59], [60], [61], [62], [63], [67], [68], [69]).

VI.1. Assessment of Steam Generator Tube Rupture Emergency Procedure (EOP) in a Single Loop PWR

This very first application involved DYLAM-TRETA-HOI with capability for automatic unfolding of the event tree (see [14], [15], [16]), and aimed at assessing the maintenance of adequate sub-cooling margin (i.e., distance to saturation conditions along the primary circuit) in the scenario of Steam Generator Tube Rupture in Jose Cabrera NPP. Without attempting here to explain the details, Figure 11 shows on the left-hand axis the sub-cooling margin evolution through the different sequences, and in the right-hand axis the evolution of the procedure steps. The operator was assumed to behave as an automatic pilot since the focus of the analysis was in the adequacy of the procedure. It may be seen both, the branching of the different sequences and the cycling of the procedure steps in some of them. For these sequences we found that the goal of the first part of the procedure, i.e., lowering the pressure in order to connect the Residual Heat Removal (RHR) system, could not be properly achieved.

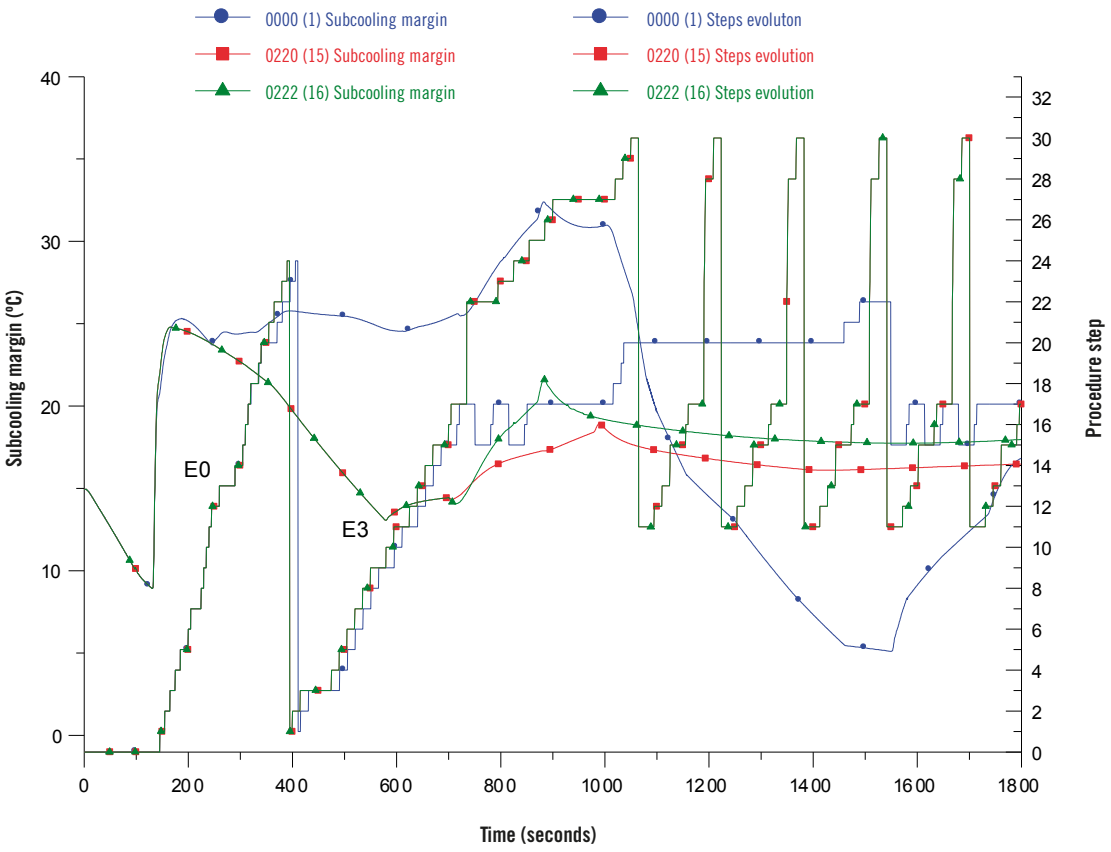

Figure 11. Assessment of SGTR EOPs: transients.

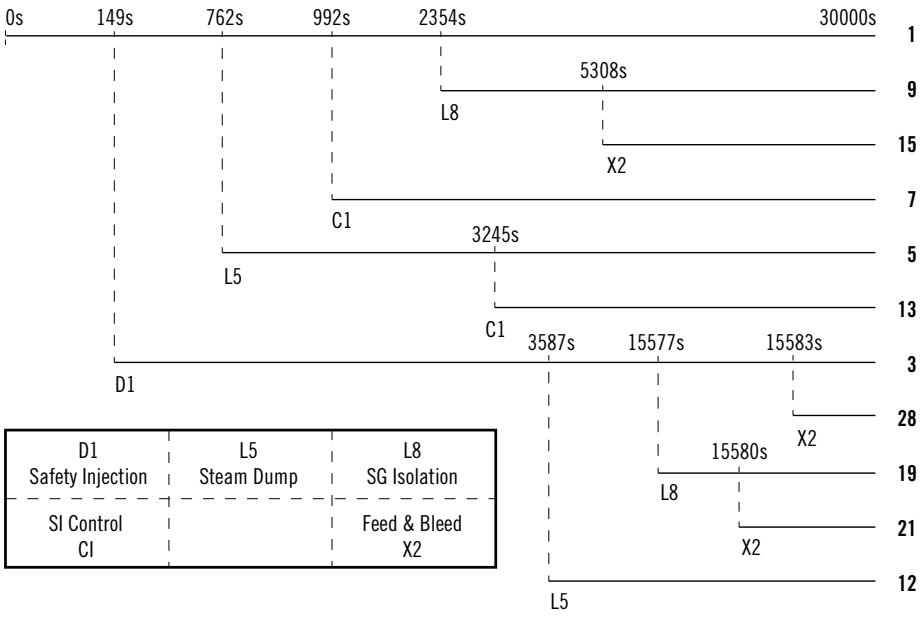

Figure 12. Assessment of SGTR EOPs: ET.

In a second step the analysis assessed the actual PSA sequence of events thorough the comparison with the Dynamic Event Tree (DET) obtained using the capability of automatic delineation of ET (tree simulation). Additionally, the phenomenology was enlarged, allowing for simulation of two-phase phenomena by replacing TRETA with the MAAP code (see [17], [18], [19]). Figure 12 shows the times at which the different events in the event tree were found to occur. Some sequences did not coincide with the ones presented by the utility and licensing actions to resolve discrepancies were taken. Among them, several changes in the emergency procedures were identified and required.

Other Safety Limit Event Trees for SGTR Sequences in a PWR-W 3 Loop Plant

The acceptance criteria used in Level 1 Probabilistic Safety Assessment (PSA) are usually related with fuel failure indicators, as the scope of Level 1 PSA is to calculate the core damage frequency. In this approach, the core damage is the first and necessary step in a potential radiological release, the containment failure being the second one. Nevertheless, Steam Generator Tube Rupture (SGTR) sequences in Pressurized Water Reactors are able to release large quantities of radioactive products without previous core damage or containment failure. For that reason, it seems necessary to analyze which sequences exceed the allowed offsite dose criteria prior to the core damage criterion.

The aim of this analysis was to evaluate the contribution to the risk of both the offsite dose and the core damage in case of SGTR sequences at full power in a 3-loop PWR Westinghouse design. The study implements the premises of ISA methodology, by using SCAIS-MAAP and RADTRAD codes (see [67], [68], [69]). For that purpose, the analysis unfolds the SGTR Dynamic Event Tree (DET) for both the core damage and the offsite dose risk metrics. The results indicate that dose criteria complement the PCT criterion and allow quantifying both risk contributions in SGTR sequences.

The sequence begins with a breach in the barrier between the primary Reactor Coolant System (RCS) and the secondary side of the steam generator (SG), providing a direct release path for RCS fluid to the environment via the secondary side (steam-dump, safety and relief) valves. The classical main recovery stages of SGTR sequences are:

1. Reactor trip and Safety Injection (SI) signal.
2. Identification and Isolation of the ruptured SG.
3. Cool-down of the RCS by means of the intact SGs.
4. Depressurization of RCS to restore inventory.
5. Termination of SI.
6. Long term cooling.

Generic headers for these are firstly obtained from SGTR event trees (ET) of PSA studies of similar NPPs. This allows to identify relevant human actions within Emergency Operating Procedures (EOPs), related to items 2 to 6 of previous list, thereafter used in DET delineation.

This study considers that SCRAM, the Auxiliary Feed-Water System (AFW) and High Pressure Recirculation (REC-HP) accomplish with their respective success criteria. In addition it does not cover RWST refill (Refueling Water Storage Tank) and RHR phases of the accident. Therefore, the considered headers are:

- H (High Pressure Injection system),
- I (Isolation of ruptured SG),
- SD (RCS cool-down at maximum rate),
- LD (RCS cool-down at 55 K/h), and
- R (SI termination).

All headers have two possible states (success or failure), except header H where three states are considered: availability of 2 trains, 1 train or 0 trains.

In summary, twenty four operator actions, corresponding to EOPs namely E-3, ES-3.1, ECA-3.1 and ECA-3.2, have been included in DET simulation. As in classic PSA, the sequences included in the DET reach a final state (either success or damage); nevertheless in this analysis such final state depends simultaneously on three possible damage criteria: Peak Cladding Temperature (PCT) limit, dose limit in Exclusion Area Boundary (EAB), and dose limit in Low Population Zone (LPZ). The PCT damage criterion refers to the classical ECCS acceptance criteria from 10 CFR 50 (PCT ≤ 1477 K at every moment) while dose limits refer to TID-14844 methodology (see [67], [68], [69]): 0.25 Sv to the whole body or 3 Sv to the thyroid, both for the critical individual for a 2-hour staying within EAB and an 8-hour staying within LPZ.

PCT evaluation depends directly on SCAIS-MAAP simulations, and dose estimation has been obtained by RADTRAD (taking as input data some MAAP results), and considering the standard meteorological conditions included in typical Safety Analysis Reports (SAR).

Main results coming up from DET simulation are depicted in Figures 13 and 14 and summarized in Tables 1 and 2, where sequences are named by the concatenation of each header status: a header in upper case means success upon demand and lower case means failed upon demand.

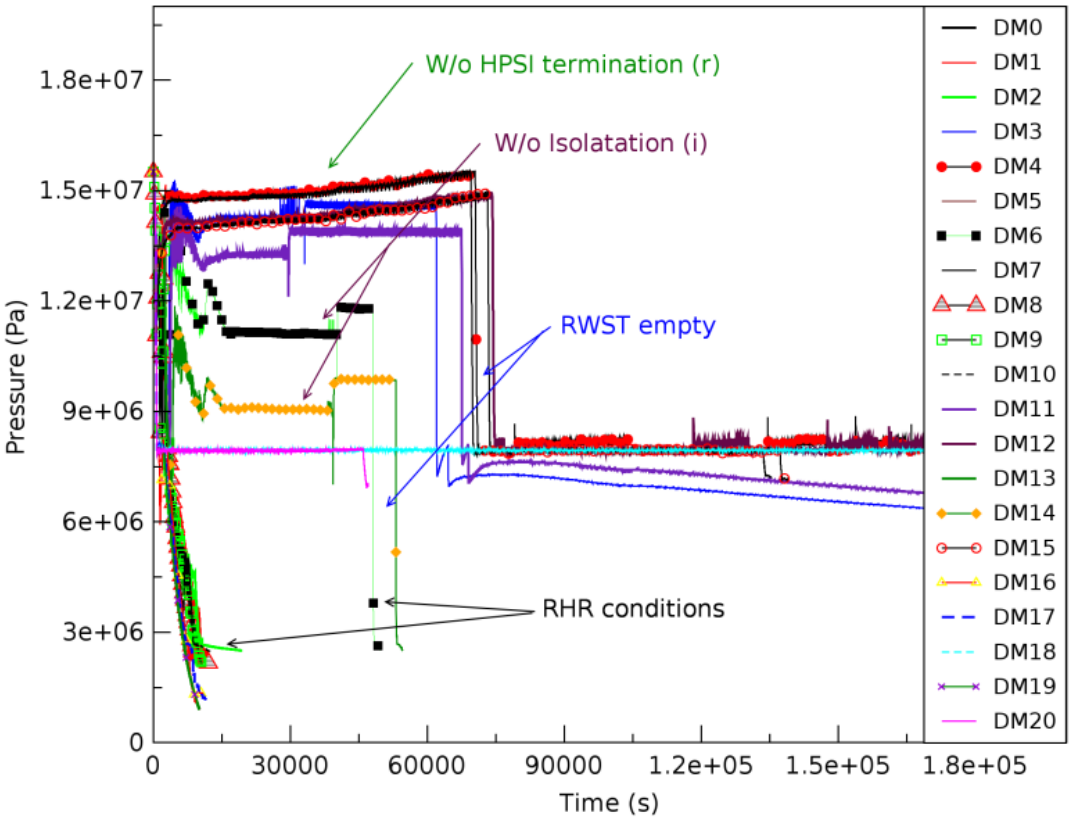

Figure 13. RCS pressure. SGTR DET.

Results from RADTRAD code (Table 2) show that the most conservative case corresponds to the dose to thyroid for the Concurrent Iodine Spike. Due to that, all values presented in Table 2 correspond to ratio between estimated dose and dose limit to the thyroid, which is 3 Sv, as previously stated. For dose calculation obtained by RADTRAD it is necessary to have the mass flow rate evolution in tube rupture and the end time of release from affected SG. DET results (see Table 2 and Figures 13 and 14) show that PCT damage end status (red color) is reached for sequences DM7, DM15 and DM20, and that dose damage end status (orange color) is reached for sequences DM3, DM4, DM6, DM11, DM12 and DM14.

Sequence	RHR conditions time (s)	End RWST time (s)	Integrated SGTR mass flow (kg)	Release ending time (s)
DM0:2HICR	12564	-----	4.50E+04	2665
DM1:2HICr	-----	61805	1.45E+05	8162
DM2:2HIcSR	19422	-----	5.40E+04	2914
DM3:2HIcSr	----	61969	1.40E+05	7790
DM4:2HIcs	----	70513	1.40E+06	69560
DM5:2HiSR	10071	-----	9.30E+04	10071
DM6:2HiSr	49714	48027	1.40E+06	49714
DM7:2His	-----	69576	1.60E+06	130306
DM8:1HICR	12053	-----	4.10E+04	2378
DM9:1HICr	----	-----	4.30E+04	2670
DM10:1HIcSR	12067	-----	1.40E+05	8716
DM11:1HIcSr	----	67509	1.40E+05	9134
DM12:1HIcs	----	74264	1.45E+06	76811
DM13:1HiSR	9981	-----	9.10E+04	9981
DM14:1HiSr	54576	53111	1.40E+06	54576
DM15:1His	-----	73215	1.60E+06	137300
DM16:0HIC	10380	-----	1.40E+04	996
DM17:0HIcS	11513	-----	1.30E+04	995
DM18:0HIcs	-----	-----	1.30E+04	995
DM19:0HiS	10132	-----	5.20E+04	10131
DM20:0His	----	-----	1.50E+05	45982

Table 1. Sequence information obtained from the DET (SCAIS/MAAP code).

Sequence	PCT (K) [damage time]	EAB(2h) Dose/Limit	LPZ(8h) Dose/Limit
DM0:2HICR	603	0.7050	0.3556
DM1:2HICr	603	0.7050	0.3500
DM2:2HIcSR	603	0.199	0.794
DM3:2HIcSr	603	0.9453	3.9257
DM4:2HIcs	603	0.8753	3.5643
DM5:2HiSR	603	0.199	0.796
DM6:2HiSr	603	0.9987	4.2593
DM7:2His	>1500 [133000s]	1.150	4.600
DM8:1HICR	603	0.6455	0.3262
DM9:1HICr	603	0.6454	0.3205
DM10:1HIcSR	603	0.6454	0.3205
DM11:1HIcSr	603	1.1502	4.5880
DM12:1HIcs	603	1.098	4.392
DM13:1HiSR	603	0.8286	0.2964
DM14:1HiSr	603	1.1403	4.457
DM15:1His	>1500 [137000s]	1.0142	3.8997
DM16:0HIC	603	0.0716	0.0354
DM17:0HIcS	603	0.0716	0.0354
DM18:0HIcs	603	0.0716	0.0354
DM19:0HiS	603	0.2128	0.0761
DM20:0His	>1500 [46823s]	0.2128	0.7833

Table 2. Damage results for SGTR-DET sequences (SCAIS/MAAP and RADTRAD code).

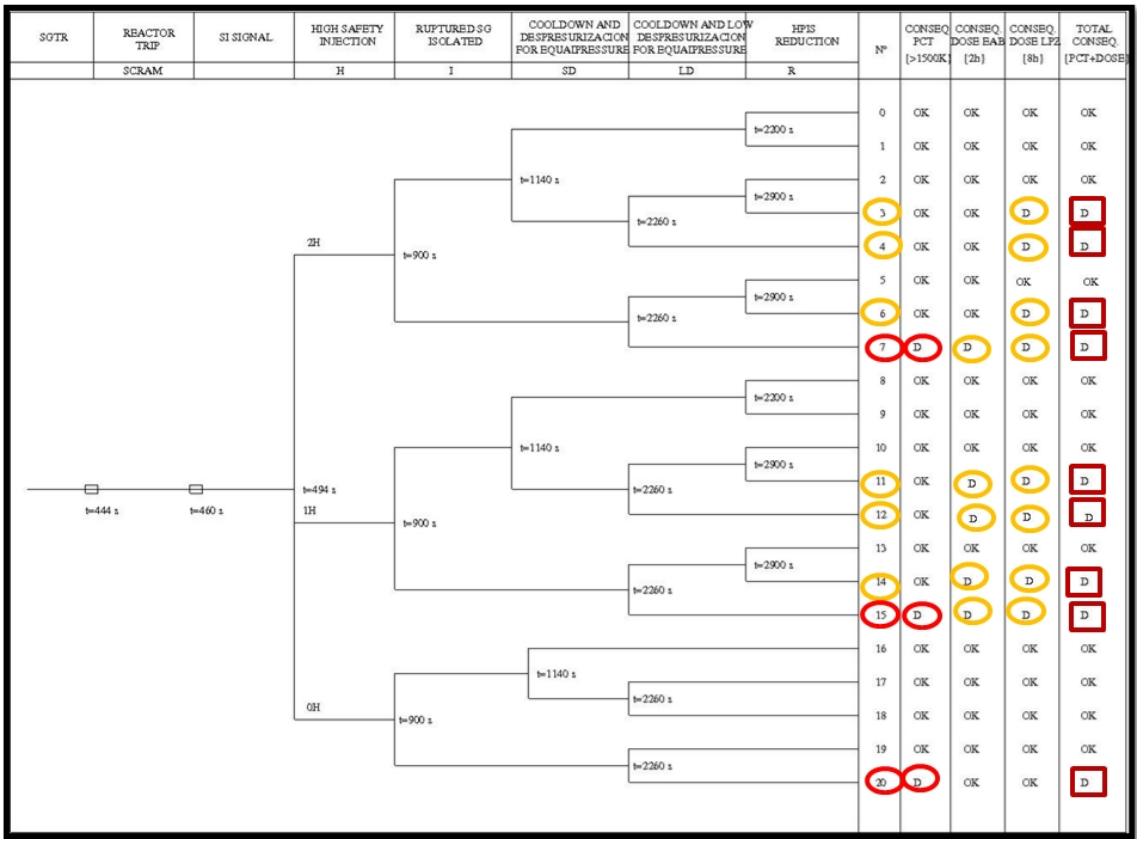

Figure 14. DET (final status includes PCT and dose criteria).

As general conclusions of this DET analysis, it is worth to note that:

- There are several sequences without PCT damage but with dose damage, and
- R header (SI termination) is a major contributor to dose damage.

These results show the adequacy of the ISA methodology to study complex safety problems, particularly those where there could appear subtle dependencies among human and systems actuation and/or process dynamics.

VI.2. SM2A-LCCW: Loss of Component Cooling System with Subsequent Reactor Pump Seal Failure in a 4 Loop PWR. Recovery of CCW

The analysis was performed with today´s SCAIS version using the MAAP wrapper and MAAP plant models in the framework of the NEA/CSNI SM2A project (see [56], [58], [59]) which developed a pilot application of the safety margin assessment methodology (see [6]). The objective was to test the SMAP method by evaluating changes in the exceedance frequency of specified safety limits as a result of a power up-rate to 110% (see [56]). CSN-UPM contribution focused on the scenario of Loss of Component Cooling Water System (LCCW), with subsequent pump seal failure in a 4 loop PWR, and analysis of delays in the recovery of CCW (see [56], [58], [59]).

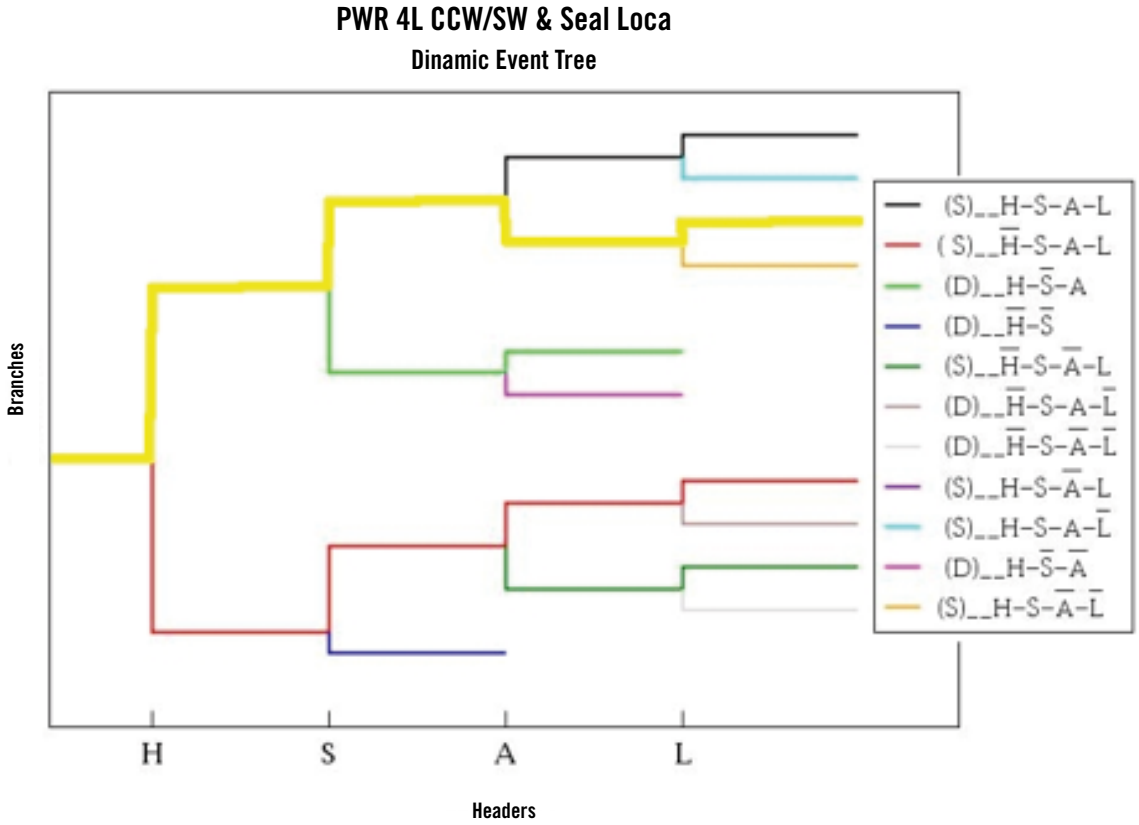

Figure 15. SM2A exercise: LCCW DET.

A pump seal failure, as any small break, would require the HPIS (high pressure injection system). However, neither the high pressure nor the low pressure safety injection (LPIS) is available without recovery of the CCW. Even if the secondary side relief system is available and may be used to manually depressurize the secondary side, its success depends on details of the two-phase situation and whether the operator action was done on time. If CCW recovery is considered, the HPIS/LPIS may recover the situation, provided it is not too late. Thus, the combination of the depressurization operator action time and the time of recovery of the CCW is to be assessed. Figure 15 shows the DET obtained automatically by SCAIS when no manual action is considered, and Figure 16 depicts the relationship between actuation times for recovery and depressurization and exceedance of the PCT (Peak Clad Temperature) safety limit. The indicated *previous damage* region represents transients where the delay in one or both actuation times is so large that the limit exceedance occurs before the intended remedial action. This illustrates that in case of operator delays (time uncertainty), whether damage occurs may only be ascertained at the transient level. Finally, Figure 17 summarizes the calculation procedure of exceedance frequency based on the TSD probabilistic model.

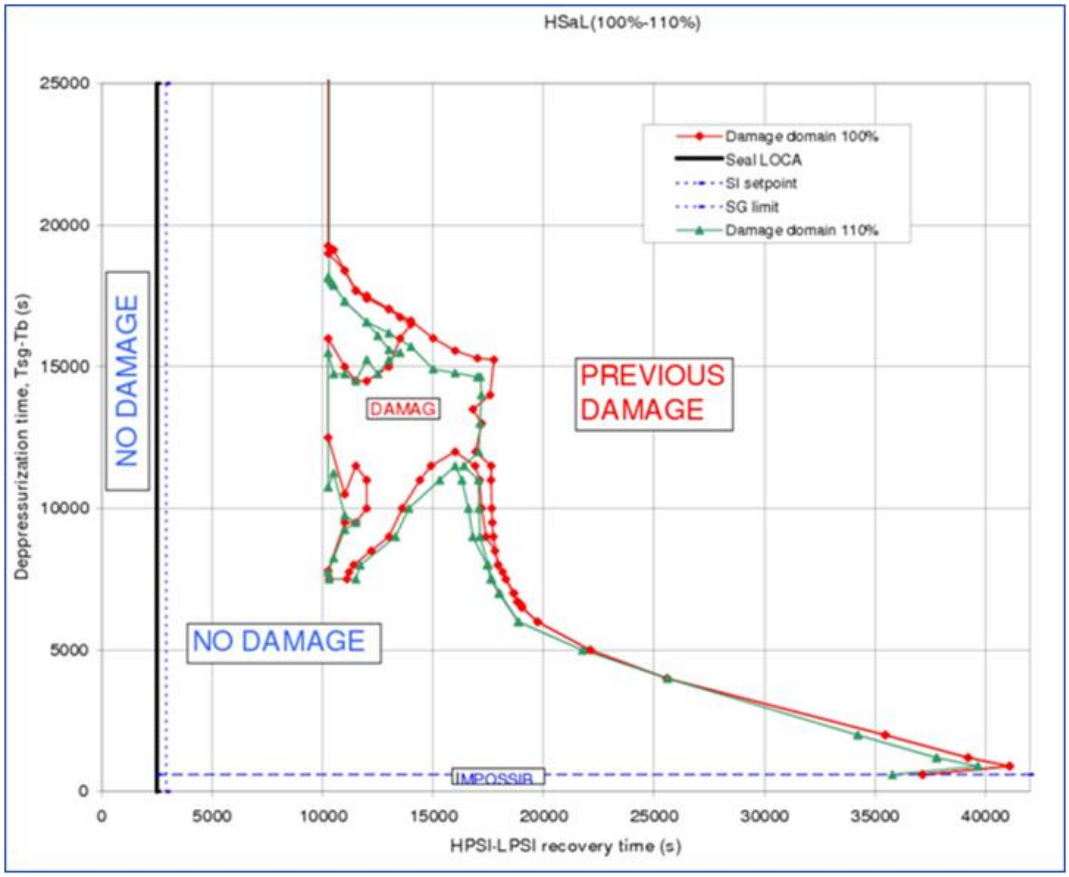

Figure 16. SM2A exercise: Damage Domain.

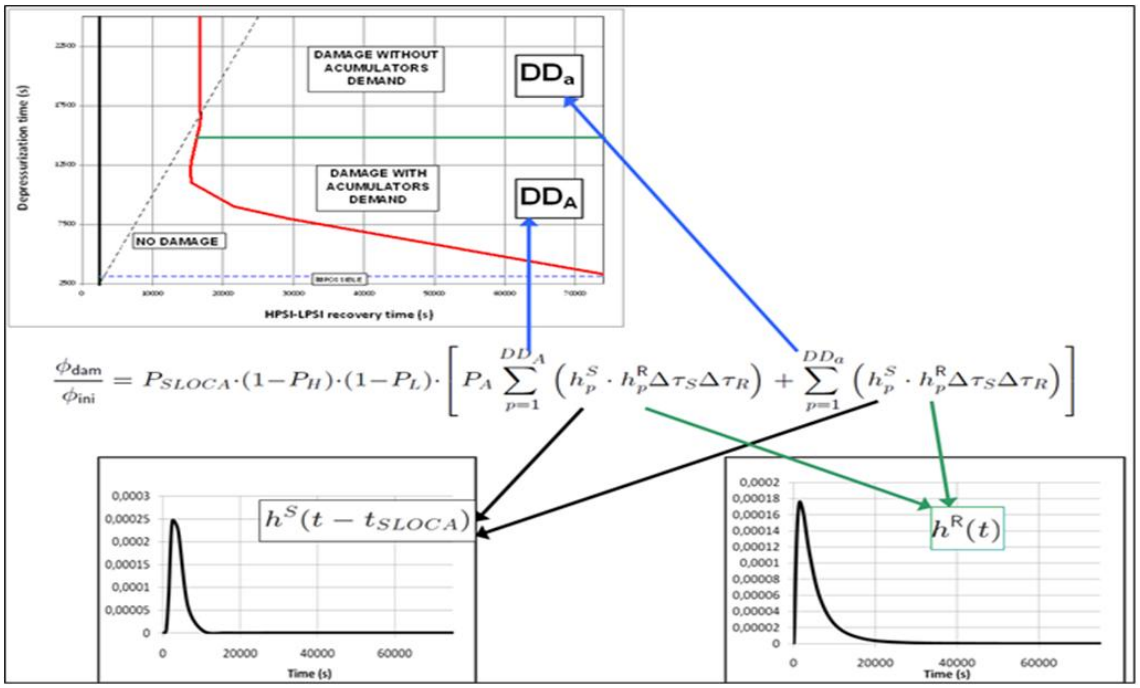

Figure 17. TSD procedure of calculating the PCT exceedance frequency.

VI.3. Dynamic Event Trees and Damage Exceedance Frequency (DEF) without Success Criteria. Application to Full Spectrum LOCA Sequences

This case[3] illustrates the potentiality of ISA approach in assessment or determination of PSA success criteria, including both system capacity and available time for human actions. It assesses the uncertainties in the break area and the operator actuation time needed to cool-down and depressurize reactor coolant system by means of steam generators in an MBLOCA scenario, without any hypotheses for success criteria (availability configurations) of stand-by safety systems (see [63], [71]). For this aim Dynamic Event Trees (DETs) for Full Spectrum Loss of Coolant Accidents (LOCAs) of a Westinghouse 3-loop PWR plant are obtained with SCAIS-MAAP, in order to obtain the Damage Exceedance Frequency (DEF) for the LOCA Event Tree.

Using the same possible headers than in a Generic Event Tree (GET), a set of DETs (for 1", 2", 3", 4", 5", 6", 7", 8", 11" and Double Ended Guillotine Break -DEGB-) are obtained taking into account all the possible availability configurations of HPSI (0-1-2/2 HPSI) and ACCUM headers (0-1-2-3/3 ACCUM). Only the classical hypothesis of availability in LPSI header (0-1/2) has been included in order to reduce the number of DET sequences.

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

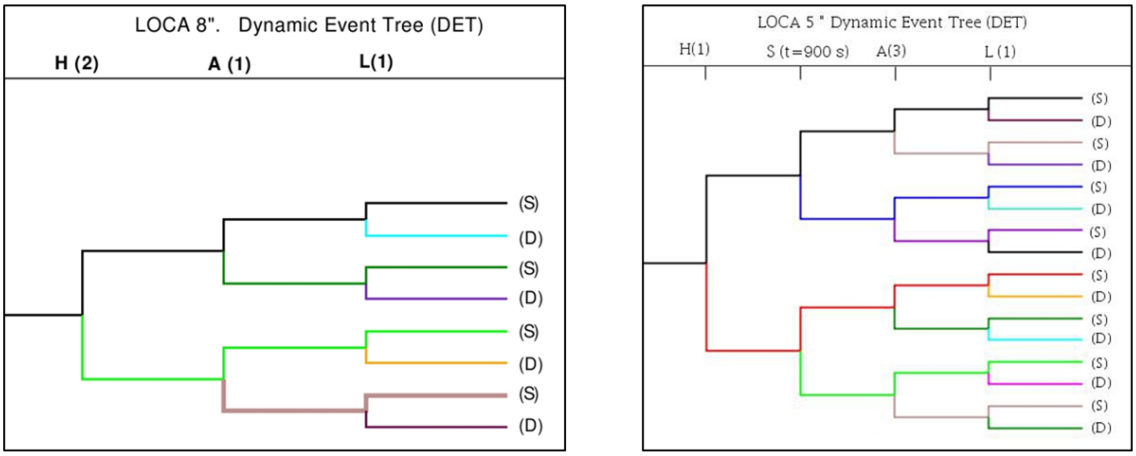

Figure 18. DETs simulation LOCA (5 and 8 inches).

During the unfolding of these DET, simulations do not consider any time delays (in this case S header occurs at t = 900 s or never). Uncertain operator action delay times are taken into account in the Path Analysis module, described in Section IV.1 above and represented by the block of the same name in Figure 4 in order to obtain the DDs, which is described below.

An example of the DETs and results for some variables obtained with MAAP-SCAIS are shown in Figures 18 and 19.

Resulting DETs have different structure depending on the break size and can be grouped by break size ranges as shown in Figure 20. Moreover, header success criteria depend also on the break size, as is shown in Figure 21, which summarizes those success criteria for headers H (High Pressure Injection System) and A (Accumulator) for different sequences and different break sizes.

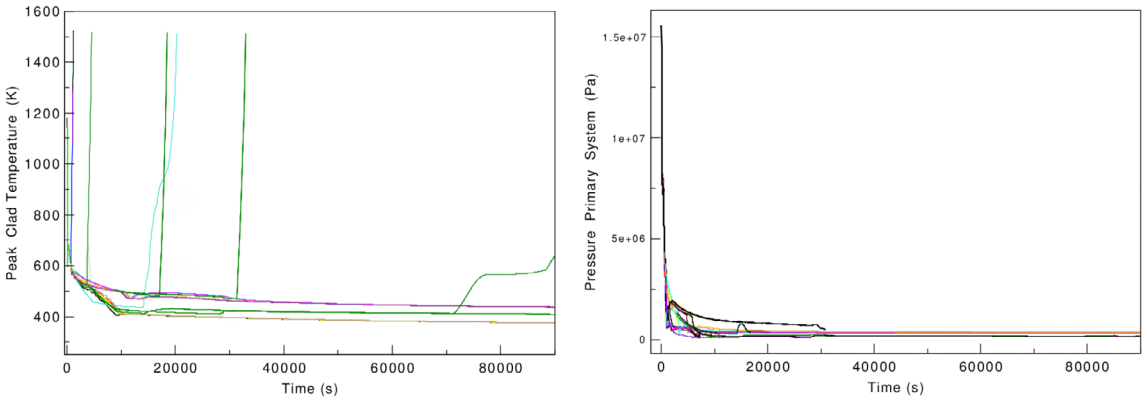

Figure 19. Pressure in RCS and PCT for every sequence of the DET (5 inches) (only 3-ACCUM results are shown in order to simplify the Figures)

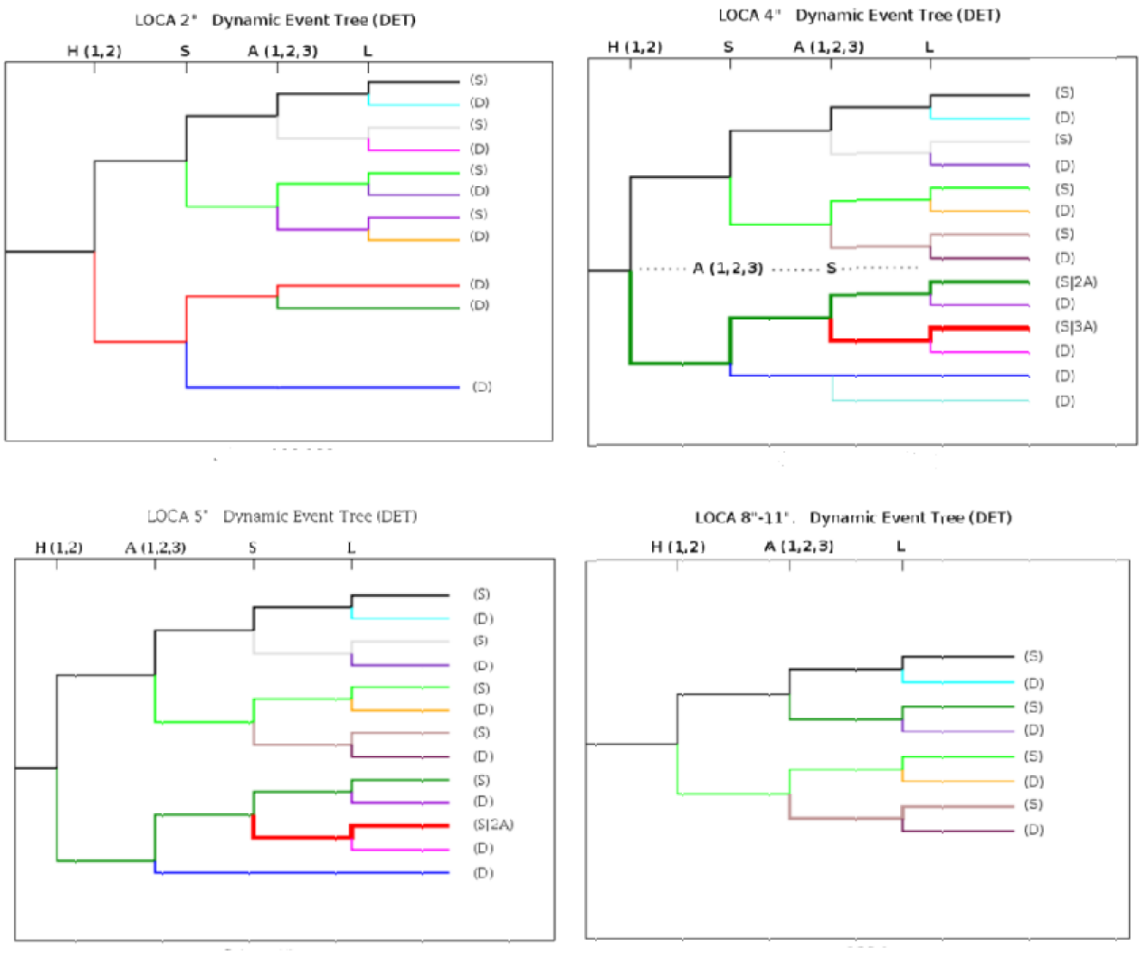

Figure 20. DETs grouped by break size.

Sequence analysis with SCAIS system allows showing that the sequence success depends on the number of available accumulators and also on the S header. Therefore, it is necessary to consider four branches for the A header (0-1-2-3 of 3 ACCUM)[4]. Also, it is necessary to take into account the time uncertainty in the S(t) header and considering the failure status of S header due to the failure of mechanical components which may prevent the success of the human action.

4. The approach is similar to the so-called Expanded Event Trees which are used in the AP1000 PSA (see [70]).

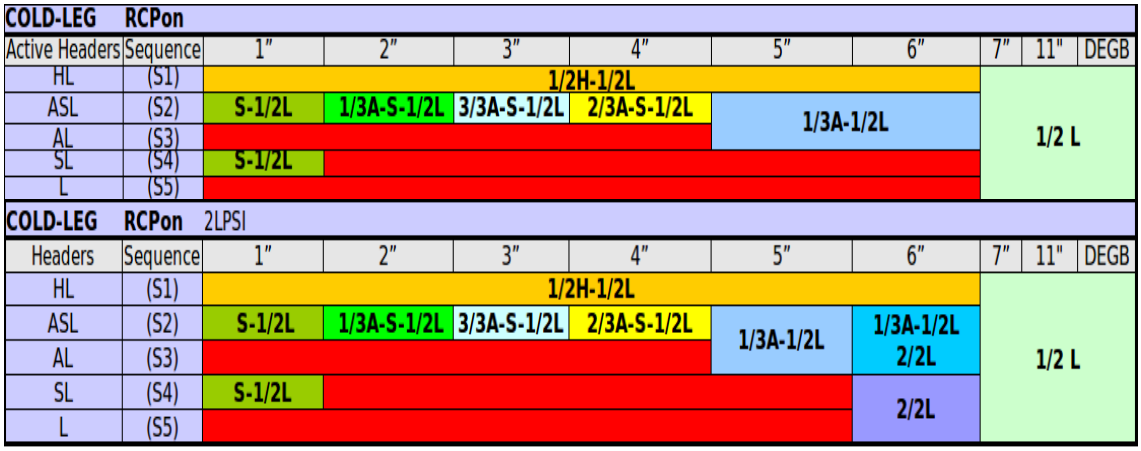

Figure 21. Success Criteria. LOCA sequences, 1 inch to DBEG. (Cold Leg, RCP trip by EOPs).

All these considerations lead to a new event tree which includes the time uncertainties and all possible system configurations named Generic Event Tree with Uncertainty (GETU), which is presented in Figure 22. The LOCA GETU shows:

I. One sequence which always has a final success state (U0),

II. Nine sequences which always have a final damage state (U1-3-5-7-9-11-13-15-17), and

III. Eight sequences in which the final state is not always success or damage (U2-4-6-8-10-12-14-16), identified in GETU (Figure 22) as sequences with Damage Domain (DD) since, for these sequences, it is necessary to obtain the DD, i.e. the time/parameter region where the paths reach the damage condition.

Since failing to execute S(t) is equivalent to infinite delay in that action, sequences U10 to U17 are actually included in sequences U2 to U9, respectively, when uncertainties are taken into account. Therefore, only the DDs of sequences U2, U4, U6 and U8 need to be obtained.

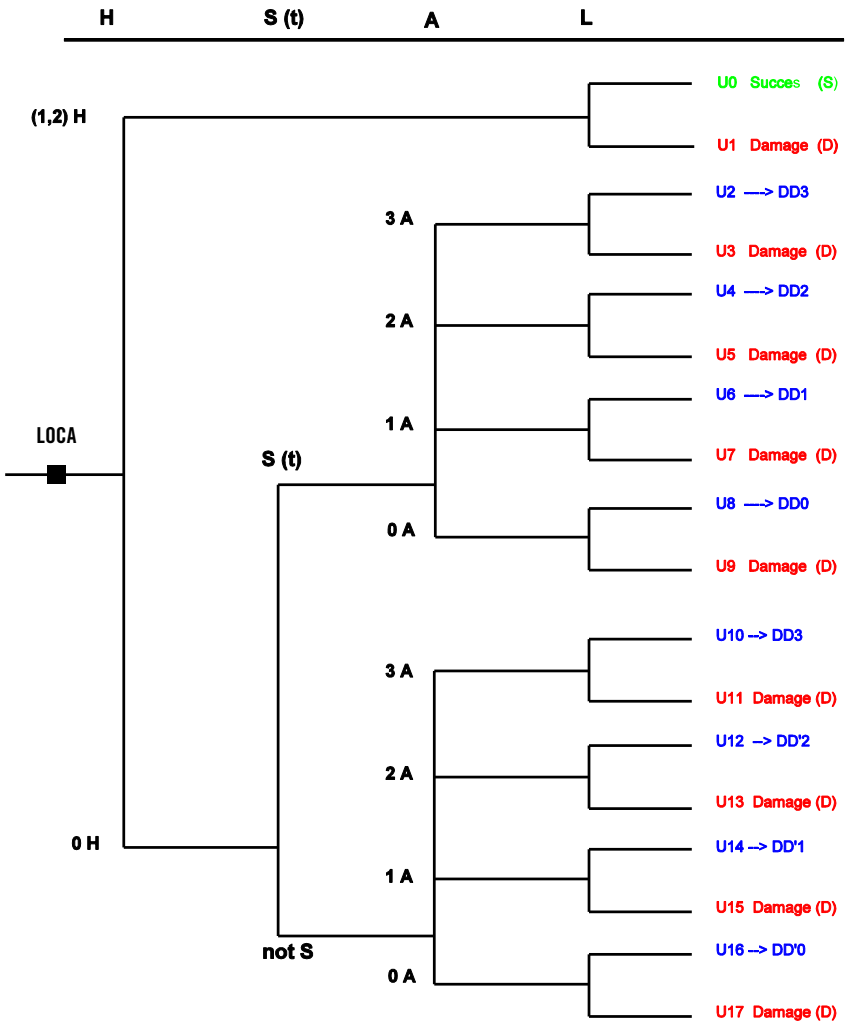

Figure 22. GETU for LOCA sequences.

The calculation process performed for each of this DD is the following:

1) For each break size and accumulators configuration, a set of paths are simulated with different operator action time delays for the start of secondary side cooling and depressurization, S(t) (see Figure 22).
2) The results are summarized using the following nomenclature of color codes, see Figure 24: green markers represent success paths, while red ones represent damage paths with ACCUM demanded and grey ones represent damage paths without ACCUM demanded. Finally, the points (d_i, $t_{0,i}$), corresponding to time $t_{0,i}$ and break diameter d_i where the damage condition (in this case maximum PCT criteria) is reached without depressurization, allows to depict the line of previous damage (dotted red line), i.e., the line corresponding to combination of uncertain parameters beyond which starting depressurization does not avoid damage.

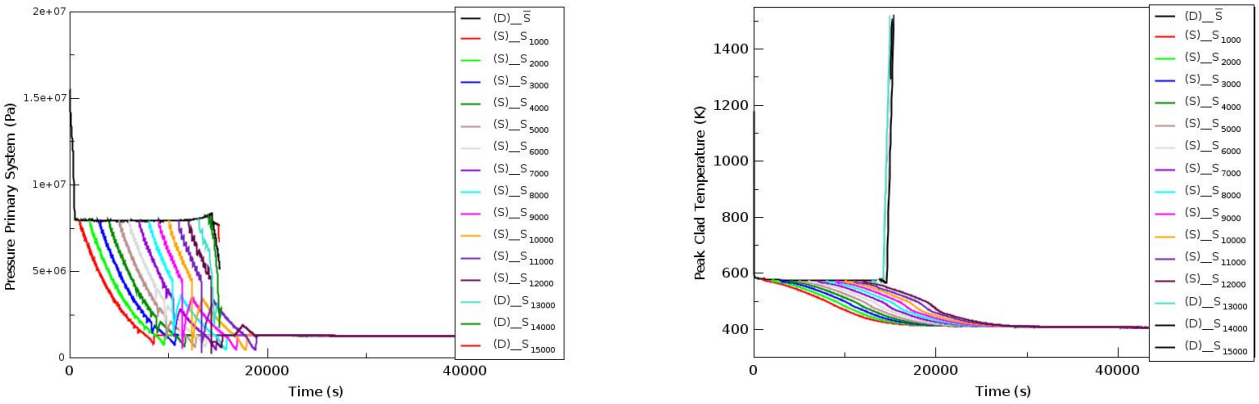

Figure 23. RCS Pressure and PCT in Path Analysis LOCA 1". (Sequence h - S(t) - (0/3A) – L)

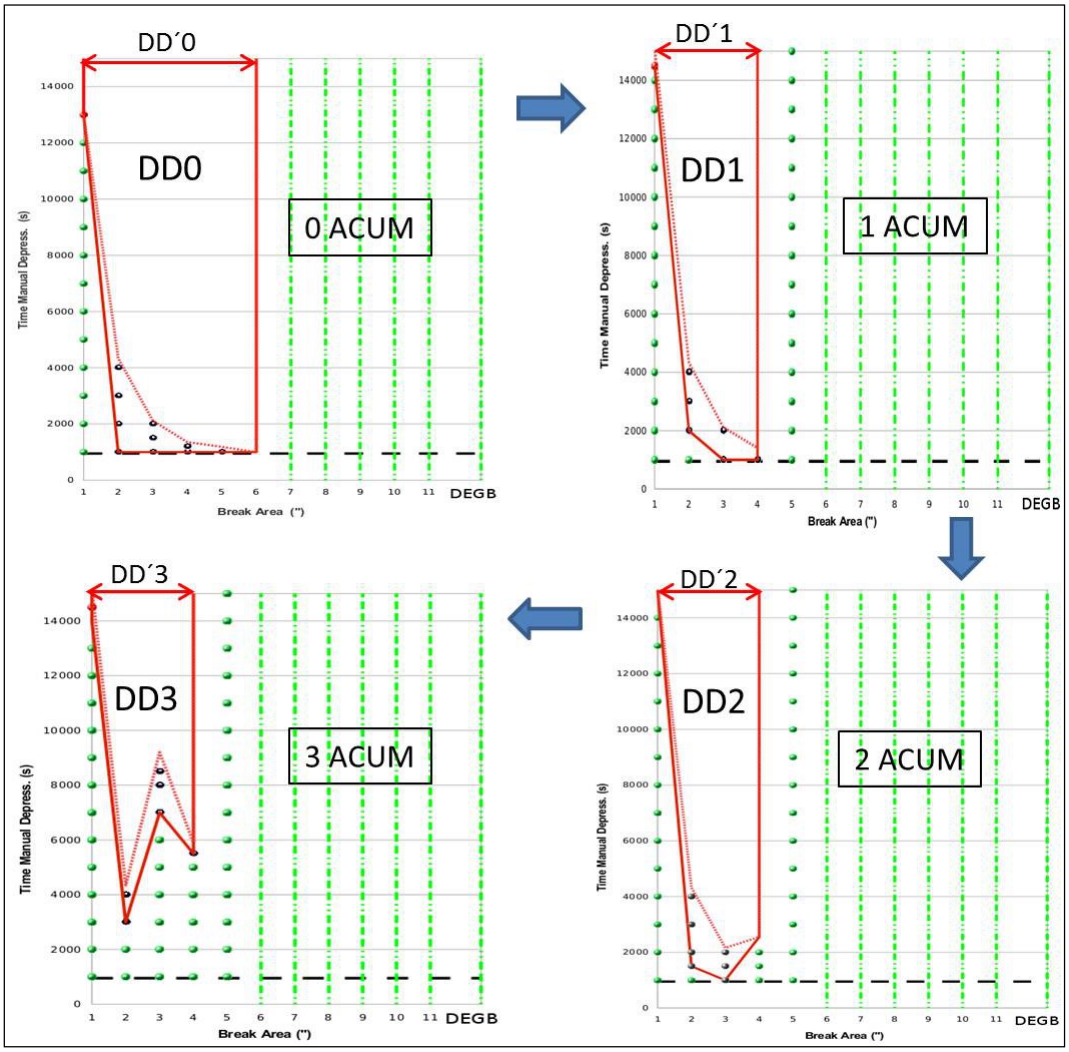

Figure 24. Damage Domains, 0/1/2/3 ACCs available. h-S(t)-(n/3)A-L sequences.

3) With these results, it is possible to obtain the DD by connecting the first depressurization time that leads to damage for each break size, red line in Figure 23. It is worth to note that there are damage paths with and without accumulator demand; this fact is taken into account to calculate probabilities/frequencies.

Combination of these results and the previous ones obtained in the Path Analysis block (see Figure 4) allows to obtain the DD and success criteria of every Ui sequence from GETU (Figure 22):

• U0 is a sequence with one-dimensional (break size) DD. H and L systems success criteria are functions of the break size as follows:

d<7"	1/2H-1/2L
d≥7"	1/2L

Sequence		Sequence Freq. (1/y)	DEF (1/y)	Rel. freq.
U0:	H-L	1,14E-03	0,000	0,000
U2:	h-S-3/3A-L	3,03E-006	2,13 E-07	0,071
U4:	h-S-2/3A-L	2,52E-006	2,32 E-07	0,092
U6:	h-S-1/3A-L	4,51E-007	4,21 E-08	0,093
U8:	h-S-0/3A-L	3,02E-008	2,96 E-09	0,098
U2/U4/U6/U8:	**h-S-L**	**2,62E-007**	**2,62E-007**	**1,000**
U10:	h-s-3/3A-L	1,21E-008	1,12E-08	0,970
U12:	h-s-2/3A-L	1,02E-008	9,51E-09	0,970
U14:	h-s-1/3A-L	1,81E-009	1,75E-09	0,970
U16:	h-s-0/3A-L	1,23E-010	1,19E-10	0,990
U10/U12/U14/U16:	**h-s-L**	**1,02E-009**	**1,02E-009**	**1,000**
U1/U3/U5/U7/U9/ U11/U13/U15/U17:	I	7,01E-006	7,01E-006	1,000
TOTAL		**1,15E-3**	**8,27E-6**	**0,007**
Cold Leg RCP trip with EOPs condition		1.15E-3	8.27E-6	0.007

Table 3. DEF of LOCA event tree.

- U2, U4, U6 and U8 are two-dimensional (break size and S actuation delay) sequences as represented in Figure 24. The respective DD are identified in this Figure as DD0, DD1, DD2 and DD3.
- U10, U12, U14 and U16 are one-dimensional (break size) sequences, that as previously indicated are included in U2, U4, U6 and U8 respectively. Their corresponding DD are qualitatively represented as DD'0, DD'1, DD'2 and DD'3 in Figure 24.

The Damage Exceedance Frequency (DEF) for each sequence of the GETU is obtained (Risk Assessment block of Figure 4, described in Section IV.1 above) from these DD integrating the TSD equations (i.e., the product of probability distribution functions) inside the DDs, by taking into account the configuration probabilities of all headers of the sequence. Table 3 summarizes results for every sequence of the event tree (see [60], [62], [63]), and illustrates that sequences can be classified not only as success or damage sequences but also as sequences with DD, meaning that they end in a success or damage state with non null complementary probabilities (sequences in blue color in Table 3).

VI.4. Effects of RCP trip when recovering HPSI during LOCA in a Westinghouse PWR

This study[5] is a good example of the possibility of using ISA as suitable method for verification of AM guidelines (EOPS or SAMGs). Current Westinghouse Emergency Operating Procedures (EOPs) indicate initially that during a Small-Break Loss-of-Coolant accident (SBLOCA), the operator must keep the Reactor Coolant Pumps (RCPs) running whenever there is unavailability of High Pressure Safety Injection system (HPSI) in order to cool the core by forced convection. However, the crew may follow different EOPs along the transient depending on its evolution. In these EOPs there are several conditions which indicate the necessity of tripping one or more RCPs when HPSI is recovered. In this analysis (see [71]) the occurrence of a SBLOCA with unavailability of HPSI has been analyzed with a model of a Spanish Nuclear Power Plant (Westinghouse 3L) for TRACE code V5.0 patch1. Two different accident management (AM) paths are considered, namely, actions included in the Optimal Recovery Guidelines (ORGs) and in Function Restoration Guidelines (FRGs), whenever the transition is required in the Inadequate Core Cooling (ICC) status tree based on RVLIS/CET instrumentation.

Following ORGs (E-0, E-1) whenever the HPSI is recovered, the RCPs should be tripped. However in some cases, damage conditions can be reached. If the RCS pressure is still far away from ACC injection (45 bar) at the time of the RCP trip, the core uncovery occurs and the RCS is not able to reach ACC injection conditions. Figures 25 to 27 show the results for a 3 in. break size with different HPIS recovery times. Once the time span of lowest core levels is obtained, different runs within such range are simulated for HPSI system recovery and RCPs trip times.

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

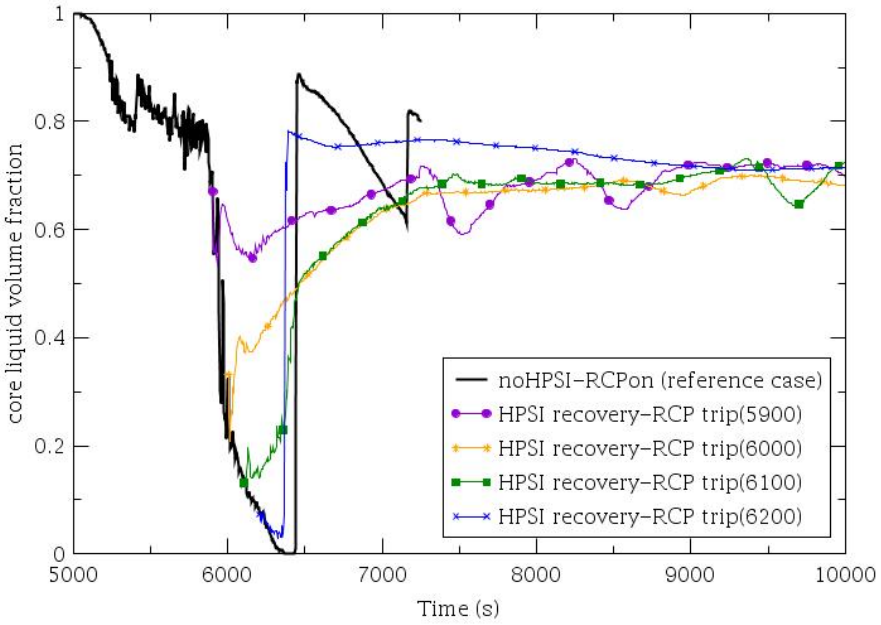

Figure 25: Core level for 3 inch SBLOCA. HPSI recovery and simultaneous 3/3 RCP trip at different times.

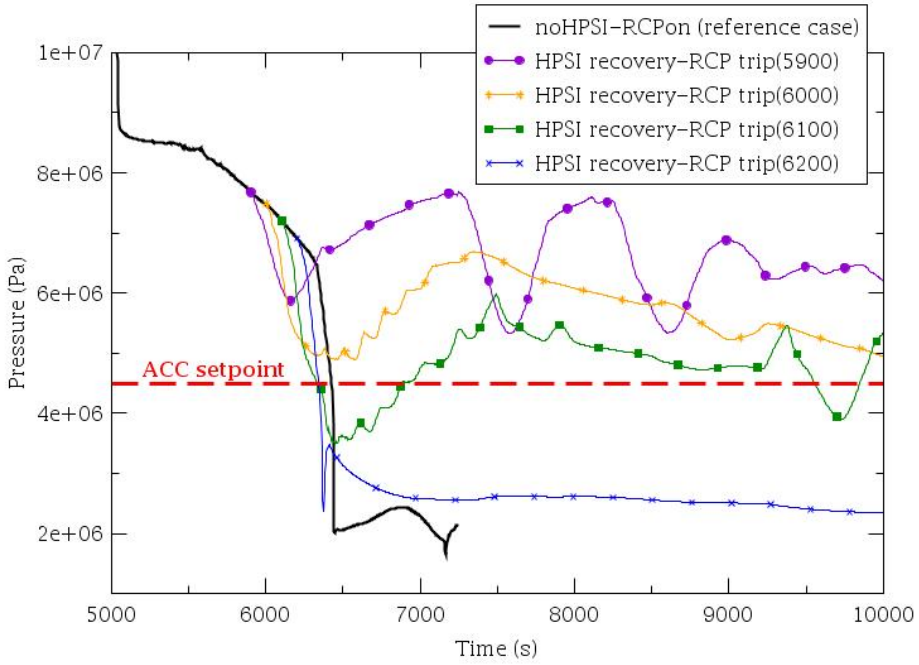

Figure 26: RCS pressure for 3 inch SBLOCA. HPSI recovery and simultaneous 3/3 RCP trip at different times.

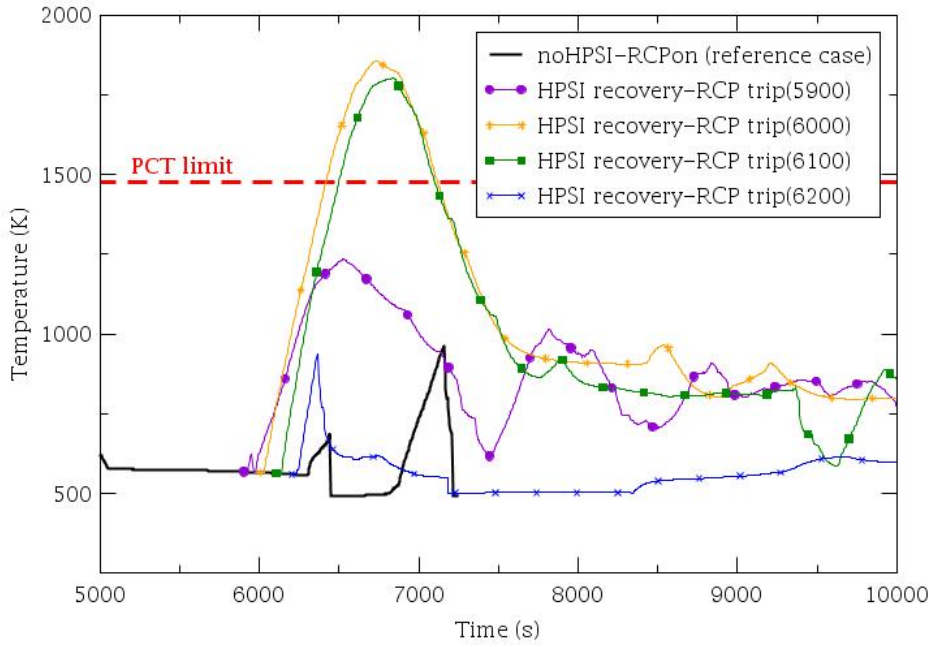

Figure 27: Peak Cladding Temperature for 3 inch SBLOCA. HPSI system recovery and simultaneous 3/3 RCP trip at different times.

Results show that there is a range between 900 seconds and 1200 seconds after the break opens, in which if the HPSI system is recovered and subsequently the RCP are tripped, the PCT limit is exceed, Figure 27.

According to these results (see [71]):

- If the HPSI system is recovered early, the core level is still high enough and the HPSI is able to recover core level. Thus, the RCP trip does not give rise to exceedance of the PCT limit.
- If the HPSI system is recovered later, there is a range in which the sequence reaches the PCT limit. The reason is that for these cases the pressure stabilizes above the ACC set-point (Figure 26, i.e., ACC cannot inject properly), and the PCT increase cannot be avoided.
- If the HPSI is recovered beyond 1200 seconds after the break occurs, the RCS pressure is low enough to allow the injection of the accumulators when the RCPs are tripped and therefore the core level is rapidly recovered.

The analysis of a wide range of break sizes and HPSI recovery times allows identifying the Damage Domain (DD), (Figure 28) and a boundig area (Figure 29) in the space of the uncertain parameters, i.e., the break size and the HPSI recovery and RCP trip time. Figure 29 identifies regions of PCT values around the DD. The time at which damage is reached, is longer for smaller sizes than for greater break sizes since the depressurization through the break is achieved far more slowly. For this reason there exists a limit of break size beyond which, the depressurization

is so rapid that the accumulators can inject before the temperature rise (4.25 inch). It is also appreciable that, if the RCP trip is performed before the ACC injection curve, the PCT limit could be exceeded.

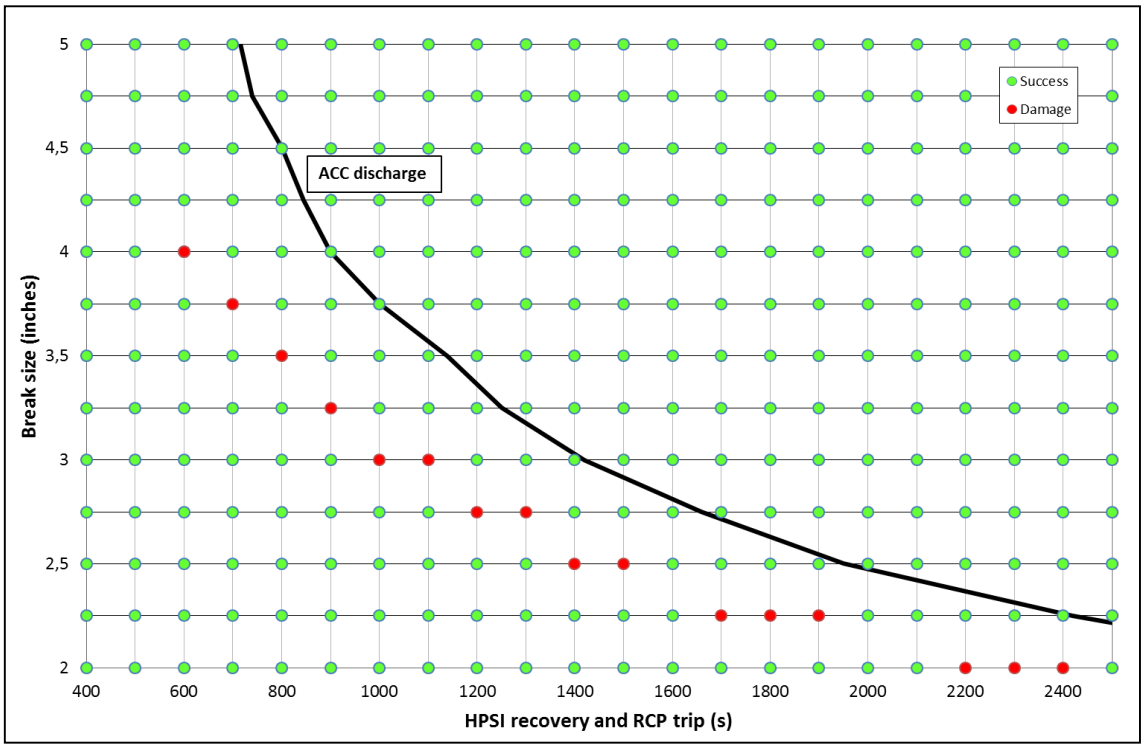

Figure 28: Damage Domain obtained for different break sizes and HPSI system recovery/RCP trip times.

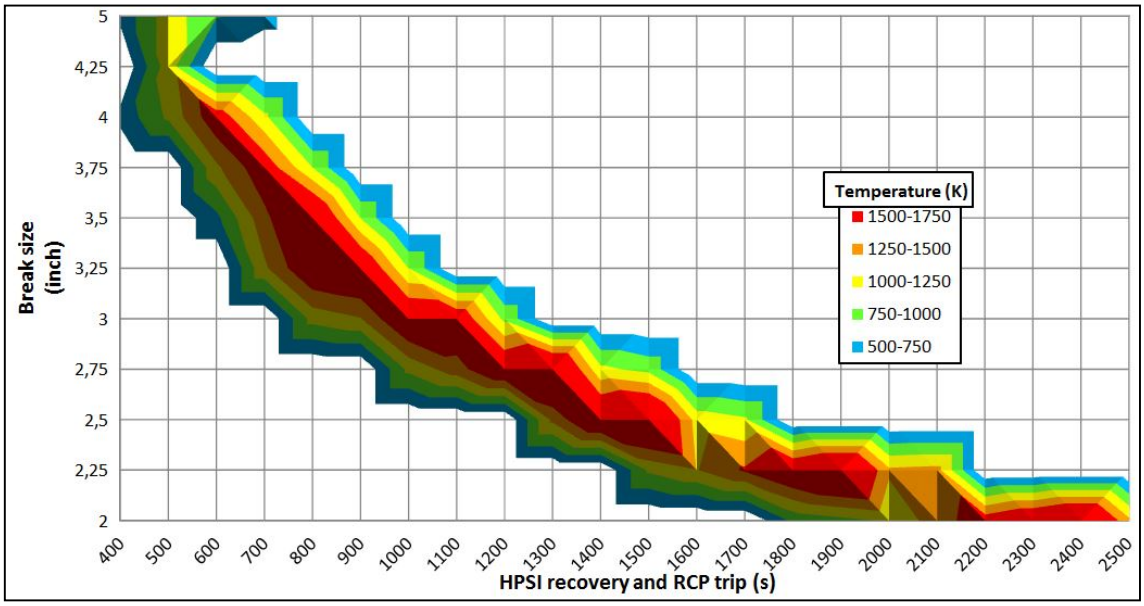

Figure 29: PCT for different break sizes and HPSI recovery and 3/3 RCP trip times.

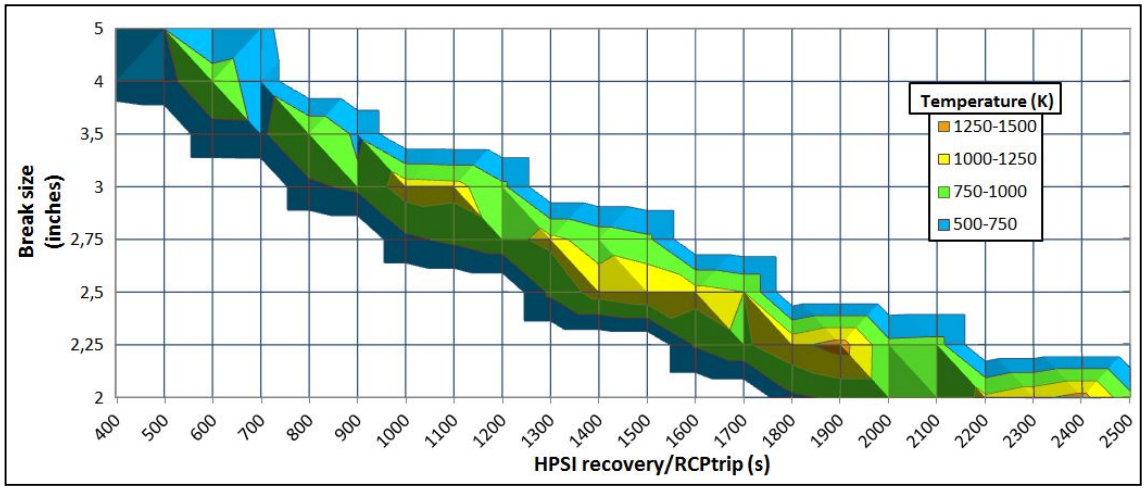

Figure 30: PCT for different break sizes and HPSI recovery and 2/3 RCP trip times (RCP broken loop is kept on).

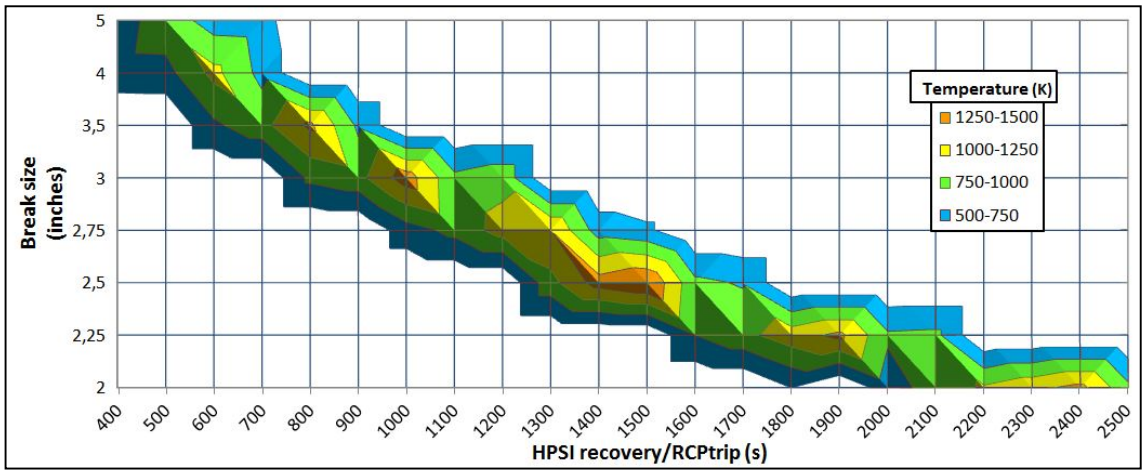

Figure 31: PCT for different break sizes and HPSI recovery and 2/3 RCP trip times (RCP broken loop is kept off).

For theses cases in which the PCT limit is exceeded, tripping two out of three RCPs has been considered as an alternative option to that of ORGs, trying to optimize the AM strategy in order to reduce the possibility of reaching damage conditions. In such case the RCP which remains running is able to cool-down the core by forced convection until the ACC can inject properly. As a consequence, in no case the PCT limit gets exceeded, as shown in Figures 30 and 31.

If RVLIS (Reactor Vessel Level Indication System) is available as ICC instrumentation, the transition to FRG, due to low core level, is considered. After the trip of the loop-2 RCP as stated in FR-C.2, the trip of the remaining RCPs produces core damage if the trip is not performed after successful injection from ACCs.

The analysis proposes two possible improvements for W EOPs corresponding to ORGs E-0 and E-1 as well as for FR-C.2, in order to avoid situations in which the PCT limit can be exceeded in the SBLOCA management (see [71]).

VII. Conclusions

VII. Conclusions

We have shown that strong evidence exists to advocate for development of diagnosis tools/ methods specific for TSO and nuclear safety regulatory bodies tasks since they should perform their own computerized analysis to verify quality, consistency, and conclusions of day to day industry safety assessments.

This helps much in a technically objective regulatory decision-making since consistency of probabilistic and deterministic aspects can be better addressed.

The document has elaborated on

1. The steps done in the development of the Integrated Safety Assessment (ISA) software package (SCAIS) and methodology used at present by the Area of Modeling and Simulation at CSN. The method couples, at each simulation time step:
   a. the simulation of trees of nuclear accident sequences resulting from consideration of potential equipment degradations following some initiating event,
   b. the sequence probability calculations and risk integration approach, and
   c. the simulation of operator actions.
2. Recent applications of the methods and tools that illustrate its potentiality to verify consistency of deterministic and probabilistic licensing safety cases, such as:
   a. Assessment of completeness of Event Tree delineation,
   b. Verification of Emergency Operating Procedures,
   c. Safety Margin Assessment,
   d. Assessment of PSA Success Criteria, including available times for operator actions.

This Volume I has focused in activities in the deterministic side, while a future Volume II will summarize the overall approach and provide similar information in the probabilistic side.

VIII. References

VIII. References

1. IAEA-TECDOC-1570, "Proposal for a Technology-Neutral Safety Approach for New Reactor Designs, September 2007.
2. "Framework for Development of a Risk-Informed, Performance–Based Alternative to 10-CFR part 50", NUREG-1860 (volumes 1 and 2), December 2007.
3. Proceedings of "SMIRT 17-Post conference Seminar 15: Optimizing Plant Safety and Operation Using a Blend of Probabilistic and Deterministic Methods", 2003 in Munich.
4. Proceedings of IAEA Topical meeting on "Advanced Safety Assessment Methods for Nuclear Reactors" in Daejon (Republic of Korea).
5. "Goals, progress and difficulties with regard to the development of German nuclear standards on the example of KTA 2000", Dr. M. Mertins, (GRS). EUROSAFE Forum 2003, Paris.
6. TASK GROUP ON SAFETY MARGINS ACTION PLAN (SMAP). Safety Margins Action Plan. Final Report. NEA/CSNI/R(2007)9. http://www.oecd-nea.org/nsd/docs/2007/csni-r2007-9.pdf. Safety Margin Assessment and Application - Final Report. NEA/CSNI/R(2011)3. http://www.oecd-nea.org/nsd/docs/2011/csni-r2011-3.pdf.
7. Izquierdo J.M. et al. (CSN), "An Integrated PSA Approach to Independent Regulatory Evaluations of Nuclear Safety Assessments of Spanish Nuclear Power Stations". EUROSAFE Forum 2003, Paris.
8. Izquierdo J.M. et al., "TRETA and TIZONA Fast Running Thermal-Hydraulic Codes", Annals of Nuclear Energy 34 (2007) 533–549.
9. Izquierdo J.M., Hortal J., Pelayo F., Pérez J., Rey J.M., Veci L., Sánchez M., "TRETA: a General Simulation Program with Application to Transients in NPPs", XIII Meeting Spanish Nuclear Society, October 1987.
10. Queral J. C., Meléndez E., Izquierdo J. M., Hortal J., Sánchez M., Herrero R., "TIZONA: A Computer Code with an Advanced Two Phase Thermal-Hydraulic Package", M&C'99 conference, Madrid 1999.
11. Cojazzi G., Meléndez E., Izquierdo J.M., Sánchez M., "The Reliability and Safety Assessment of Protection Systems by the Use of Dynamic Event Trees. The DYLAM-TRETA Package". *Proc. XVIII Annual Meeting Spanish Nuclear Society*, Puerto de Santa María, Spain, 28-30 October 1992.
12. Izquierdo J.M., Sánchez M., "DYLAM-TRETA: An Approach to Protection Systems Software Analysis", in Advanced Systems Reliability Modeling, Proc. *Ispra course held at ETSI Navales*, Madrid, Spain, September 1988.
13. Izquierdo J.M., Sánchez M., Cacciabue P.C., "Dynamic Reliability as a Tool for the Assessment of Protection Systems Software Analysis", presented at the NUCSAFE ENS/ANS Conference, Avignon, France, October 1988.

14. Izquierdo J.M., Hortal J., Meléndez E., Sánchez M., Automatic Generation of Dynamic Event Trees: a Tool for Integrated Safety Assessment (ISA). *In Reliability and Safety Assessment of Dynamic Process Systems,* (eds T. Aldemir et al.), NATO ASI series F, vol. 120, Berlin, Springer Verlag, Berlin, 1994. *Reliability Engineering & System Safety,* 52 (1996).
15. Izquierdo J.M., Sánchez M., "Application of the Integrated Safety Assessment Methodology to the Emergency Procedures of a SGTR of a PWR", *Reliability Engineering & System Safety,* 45 (1994) 159-173.
16. Sánchez M., Melara J., "Extending PSA to Accident Management. The Case of the Steam Generator Tube Rupture (SGTR) Emergency Operating Procedures Assessment", *International Conference on Nuclear Engineering (ICONE-IV) ASME meeting.* New Orleans, March 10-14 1996.
17. Izquierdo J.M., Queral C., Herrero R., Hortal J., Sánchez M., Meléndez E., Muñoz R., "Role of Fast Running TH Codes and Their Coupling with PSA Tools", in Advanced Thermal-hydraulic and Neutronic Codes: Current and Future Applications. NEA/CSNI/R(2001)2, Vol. 2, Workshop Proceedings, Barcelona (Spain) 10-13 April 2000.
18. Hortal J., "Simulation of Operating Procedures as a Tool for NPP Procedure Verification", Enlarged HRP meeting, Loen (Norway) 19-24th may, 1996.
19. Trillo A., Meléndez E., Sánchez M., Mínguez E., Muñoz R., Izquierdo J.M., "Analysis of the Steam Generator Tube Rupture Initiating Event", 24 Meeting of the Spanish Nuclear Society, Valladolid 14-16 de octubre de 1998.
20. Muñoz R., Mínguez E., Meléndez E., Izquierdo J.M., Sánchez M., "DENDROS: A Second Generation Scheduler for Dynamic Event Trees", M&C'99, Madrid, 1999.
21. Meléndez E., Izquerdo J.M., Sánchez M., Hortal J., Pérez-mulas A., "Tree Simulation Techniques for Integrated Safety Assessment", CSNI Specialist Meeting on Simulators and Plant Analysers, Espoo, Finland, 1999.
22. Muñoz, R., et al., "Development of Accident Sequence Precursor Methodologies for Core Damage Probabilities in Nuclear PWR Plants (NPP)", XXIV Reunión de la SNE, Octubre 1998.
23. Izquierdo J.M. et al., "SCAIS (Simulation Code System for Integrated Safety Assessment): Current status and applications", ESREL 2008 and 17th SRA Europe. Valencia (Spain), September, 2008.
24. J. Gil, I. Fernández, S. Murcia, J. Gómez, H. Marrão, C. Queral, A. Expósito, G. Rodríguez, L. Ibañez, J. Hortal, J. M. Izquierdo, M. Sánchez, E. Meléndez, "A Code for Simulation of Human Failure Events in Nuclear Power Plants: SIMPROC", Nuclear Engineering and Design, Volume 241, Issue 4, April 2011, Pages 1097-1107.
25. 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.

26. Herrero R., Izquierdo J.M., "Development of a computer tool for in-depth analysis and post processing of the RELAP5 thermal hydraulic code". NUREG/IA-0253. US Nuclear Regulatory Commission. Office of Nuclear Regulatory Research.
27. Meléndez E., "Experience with Probabilistic Event Analyses at CSN", 17th Meeting on Experiences with Risk-Based Precursor Analysis organized by BelV, Brussels, November 7-9, 2013.
28. Meléndez E., Herrero R., "Use of PSA model XML Standard Formats for V&V", The 2015 International Topical Meeting on Probabilistic Safety Assessment and Analysis (PSA2015), Sun Valley, ID, USA, April 26-30, 2015.
29. Ibáñez-llano C., Meléndez E., Nieto F., "Variable Ordering Schemes to Apply to the Binary Decision Diagram Methodology for Event Tree Sequences Assessment", European Safety & Reliability Association Conference (ESREL'06). Portugal, 18-22 September 2006.
30. Ibáñez-llano C., Rauzy A., "Variable Ordering Heuristics for BDD based on Minimal Cut-Sets", International Probabilistic Safety Assessment and Management Conference (PSAM9). China, 18-23 May 2008.
31. Ibáñez-llano C., Rauzy A., Meléndez E., Nieto F., "Variable Ordering Techniques for the Application of BDD on PSA linked Fault Tree Models", European Safety & Reliability Association (ESRA) and 17th Society for Risk Analysis Europe (SRA-E) Conferences (ESREL'08). Spain, 22-25 September 2008.
32. Ibáñez-llano C., Meléndez E., Nieto F., "Variable Ordering Schemes to Apply to the Binary Decision Diagram Methodology for Event Tree Sequences Assessment", Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. vol. 222, no. 1, pp. 7-16, January 2008.
33. Ibáñez-llano C., Rauzy A., Meléndez E., Nieto F., "Minimal Cut-Sets based Reduction Approach for the Use of Binary Decision Diagrams on Probabilistic Safety Assessment Fault Tree Models", Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability. vol. 223, no. 4, pp. 301-311, December 2009.
34. Ibáñez-llano C., Rauzy A., Meléndez E., Nieto F., "Hybrid Approach for the Assessment of PSA Models by Means of Binary Decision Diagrams", Reliability Engineering and System Safety. Vol. 95, Issue 10, October 2010, Pages 1076-1092
35. Ibáñez-llano C., Rauzy A., Meléndez E., Nieto F., "A Reduction Approach to Improve the Quantification of Linked Fault Trees through Binary Decision Diagrams", Reliability Engineering and System Safety. Special Issue of Selected Papers from ESREL 2008, June 25 2010. http://dx.doi.org/10.1016/j.ress.2010.06.008
36. Ibáñez-llano C., "Application of the Binary Decision Diagrams to the Integrated Safety Assessment", PhD thesis, IIT, Escuela Técnica Superior de Ingenieros Industriales, UPCo, September 2010.

37. Aldemir T. et al., "Reliability and Safety Assessment of Dynamic Process Systems", Proceedings of the NATO Advanced Research Workshop on Reliability and Safety Assessment of Dynamic Process Systems, held in Kusadasi-Aydin, Turkey, August 24-28, 1992.
38. Devooght J., Smidts C., 1992a, "Probabilistic Reactor Dynamics (I). The Theory of Continuous Event Trees", Nucl. Sci. Eng. 111, 229-240.
39. Smidts C., Devooght J., 1992b, "Probabilistic Reactor Dynamics (II). A Monte Carlo Study of a Fast Reactor Transient", Nucl. Sci. Eng. 111, 241-256.
40. Devooght J., Izquierdo J.M., Meléndez E., "Relationships between Probabilistic Dynamics and Event Trees", *Reliability Engineering & System Safety,* 52 (1996) 197-209.
41. Labeau P.E., Izquierdo J.M., "Modeling PSA problems (I). The Stimulus Driven Theory of Probabilistic Dynamics", Nuclear Science and Engineering, 150, 115–139, (2005).
42. Labeau P.E., Izquierdo J.M., "Modeling PSA problems (II). A Cell-to-Cell Transport Theory Approach", Nuclear Science and Engineering, 150, 115–139, (2005).
43. Izquierdo J.M., Cañamón I., "Conclusions of the SDTPD/TSD methods development: Results of its application to the WP5.3 benchmark Level 2 PSA", DSR/SAGR/FT 2004.074, SARNET PSA2 D117, October 2008
44. Izquierdo J.M., Sánchez M., Hortal J., Meléndez E., "A Short Description of the Integrated Safety Assessment Methodology and its Potential for Application to PSA2 problems", November 2004, SARNET portal.
45. Izquierdo J.M., Sánchez M., "Status Report on Dynamic Reliability: SDTPD Path and Sequence TSD Developments. Proposal for an enlarged step 3 exercise benchmark Level 2 PSA. The dynamic model", DSR/SAGR/FT 2004.074, SARNET PSA2 D73, September 2007.
46. Izquierdo J.M., "SARNET WP5.3 Benchmark Exercise: Application of the SDTPD Risk Assessment Approach to Assess Laminar Deflagration and Over-Pressure in a PWR Containment under Medium Break Severe Accident Conditions. Appendix 2. Benchmark simple model", CSN report. June 2005.
47. Ibáñez-llano C., "Monte Carlo Simulation Techniques Applied to Dynamic Reliability Methods. Application to a Benchmark Exercise", June 2007.
48. Izquierdo J.M., Slides of presentations at SARNET-PSA2 WP5.3 technical meetings: 3rd (Varna), 5th (Aix en Provence), and dedicated technical meeting Nov. 2005 (Cadarache), SARNET Portal PSA2 team site.
49. Izquierdo J.M., Cañamón I., "Status Report on Dynamic Reliability: SDTPD Path and Sequence TSD Developments. Application to the WP5.3 Benchmark Level 2 PSA exercise", SARNET-PSA2 WP5.3 D73. December 2006.

50. Ibañez L. et al., "Damage Domain Approach as a Strategy of Damage Exceedance Computation", Paper presented at the NENE-2009 International conference, Portoroz (Slovenia), 6-9 September, 2009.
51. Izquierdo J.M., Labeau P.E., "The Stimulus-Driven Theory of Probabilistic Dynamics as Framework for Probabilistic Safety Assessment", PSAM-7/ESREL-04 Conference, Springer, Berlin, Germany. 2004.
52. 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.
53. Sánchez M. et al., "Proposal for a Suitable Strategy of Exceedance Frequency Computation. Implementation on SCAIS Simulation-Based Safety Code Cluster", Nuclear Energy for New Europe (NENE-2009), Bled (Slovenia), 6-9 September 2010.
54. Izquierdo J.M., Galushin S.E., Sánchez M., "Transmission Functions and its application to the analysis of time uncertainties in Protection Engineering", Process Safety and Environmental Protection (2013), http://dx.doi.org/10.1016/j.psep.2013.07.004.
55. Izquierdo J.M., Paris C., Sánchez M., "The Theory of Transmission Functions and its Application to Protection Engineering", sent for publication at Process Safety and Environmental Protection (November 2015).
56. NEA Report, 2011. Safety Margin Evaluation - SMAP Framework Assessment and Application. Final Report. NEA/CSNI/R(2011)3. http://www.oecd-nea.org/nsd/docs/2011/csni-r2011-3.pdf.
57. Hortal J., Mendizábal R & pelayo F., "What does 'safety margin' really mean?" Presented at ESREL-2008 & 17th SRA Europe Annual Conference, Valencia (Spain), September, 2008.
58. Queral C. et al., "Application of the Integrated Safety Assessment to Sequences with Loss of Component Cooling Water System", The 14th International Topical Meeting on Nuclear Reactor Thermalhydraulics, NURETH-14, Toronto, Ontario, Canada, September 25-30, 2011.
59. Ibañez 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.
60. Queral C. et al., "Application of the Integrated Safety Assessment Methodology to LWR Sequences", Karlsruhe Institute of Technology (KIT) Karlsruhe, Germany, June 30th, 2011.
61. Queral C. et al., "Analysis of Surge Line MBLOCA Sequences with HPSI Failed", The 14th International Topical Meeting on Nuclear Reactor Thermalhydraulics, NURETH-14, Toronto, Ontario, Canada, September 25-30, 2011.

62. Queral C. et al., "Calculation of Damage Frequencies without Success Criteria Hypothesis. Application to MBLOCA Sequences", PSAM 2012. Helsinki, Finlandia. 2012.
63. Gómez-magán J.J. et al., "Árboles de sucesos dinámicos aplicados a secuencias Full Spectrum LOCA. Cálculo de la frecuencia de excedencia del daño mediante la metodología Análisis Integrado de Seguridad (ISA)", Revista de la Sociedad Nuclear Española, NUCLEAR ESPAÑA junio 2013.
64. Flores A., Izquierdo J.M., Sánchez M., Gallego E., "Development of an Adequate Model for Verification of Design Safety-Margins of the HTTR Nuclear Test Facility", sent to Progress of Nuclear Energy.
65. Flores A., Izquierdo J.M., Tucek K., Gallego E., "Assessment of damage domains of the High-Temperature Engineering Test Reactor (HTTR)", Annals of Nuclear Energy 72 (2014) 242–256, http://dx.doi.org/10.1016/j.anucene.2014.05.008.
66. Flores A., "Desarrollo de una Metodología de Análisis del Riesgo para Sistemas de Generación de Hidrógeno mediante Reactores Nucleares", PhD thesis, Escuela Técnica Superior de Ingenieros Industriales, Universidad Politécncia de Madrid (UPM), 2012.
67. G. Jimenez-Varas, C. Queral, M.J.Rebollo, J.C. Martínez-Murillo, E. López-Alonso. "Analysis of the operator action and the single failure criteria in a SGTR sequence using best estimate assumptions with TRACE 5.0". Annals of Nuclear Energy 58 (2013) 161–177.
68. Jiménez G., "Analisis Integrado de Seguridad de un accidente de SGTR en un reactor nuclear tipo PWR", Tesis Doctoral, ETSII-UPM, 2012.
69. Rebollo M.J. et al., "Evaluation of the offsite dose contribution to the global risk in a Steam Generator Tube Rupture scenario", Reliability Engineering and System Safety 147 (2016) 32–48, http://dx.doi.org/10.1016/j.ress.2015.10.016.
70. Sancaktar S., Schulz T., "Risk informing PRA success criteria. Application to the AP1000". In 2004 international congress on advances in nuclear power plants (ICAPP '04), Pittsburgh, PA; 2004.
71. Montero-Mayorga J., Queral C., Gonzáez-Cadelo J., "Effects of delayed RCP trip during SBLOCA in PWR", Annals of Nuclear Energy 63 (2014) 107–125.

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

CSN CONSEJO DE SEGURIDAD NUCLEAR