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

Deterministic Aspects

CSN

Colección
Otros Documentos
42.2017

CSN CONSEJO DE SEGURIDAD NUCLEAR

The importance of accident time evolution in regulatory safety assessment. Independent, quantitative tools and methods at CSN to ensure adequate PSA/DSA applications.

Deterministic Aspects.

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

Modeling and Simulation Area (MOSI), Nuclear Safety Council (CSN).

CSN CONSEJO DE SEGURIDAD NUCLEAR

Colección Otros Documentos
ODE-04.24

Edita y distribuye:
Consejo de Seguridad Nuclear
C/ Justo Dorado, 11. 28040 Madrid. España
www.csn.es
peticiones@csn.es
Maquetación: Item Multimedia S.L.
www.itemmultimedia.es
Depósito legal: M-5128-2017

Table of contents

Presentación

Presentación

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

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

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

Históricamente, el licenciamiento basado en los análisis de accidentes base de diseño siguiendo la llamada metodología determinista (DSA en sus siglas en inglés) se demostró pronto insuficiente para abordar otros aspectos de la seguridad, más relacionados con la operación que con el diseño de la planta. El accidente de Three Mile Island no hizo sino acentuar la necesidad de desarrollar los ya incipientes análisis de riesgo, comúnmente conocidos como Análisis Probabilistas de Seguridad (APS o, en inglés, PSA), no como reemplazo sino como complemento de los análisis deterministas.

La dificultad de combinar de manera adecuada la aplicación de ambos tipos de análisis manteniendo la consistencia entre ellos se ejemplifica en dos problemas de especial relevancia en

relación con la seguridad de las instalaciones:

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

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

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

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

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

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

Todo ello ha sido realizado en su mayor parte con la colaboración del Departamento de Energía y Combustibles de la Escuela Técnica Superior de Ingenieros de Minas de la UPM

(Universidad Politécnica de Madrid), y con la empresa NFQ Solutions (anteriormente, Indizen Technologies).

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

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

dedicados respectivamente a los aspectos determinista ([1]) y probabilista ([2)]. Estos documentos describen el contexto, propósito, historia, modos de uso en distintas aplicaciones, ejemplos, etc., del método ISA en sus vertientes determinista y probabilista, pero no incluyen detalles técnicos de importancia, particularmente los de modelación matemática.

Por flexibilidad documental, los aspectos de detalle del volumen I ([1]) se han editado con títulos independientes, pero pueden ser considerados como anexos. Están orientados a los usuarios del sistema informático que quieran conocer con precisión sus fundamentos y pueden ser considerados como la parte teórica de sus manuales de usuario. Contienen por consiguiente y de manera inevitable aspectos redundantes con el volumen I ([1]), pero descargan a éste de detalles que impiden una lectura más accesible.

El documento ([3]):

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

detalla esta especial aplicación al licenciamiento en la que las técnicas integradas son imprescindibles, y donde CSN-MOSI ha tenido una activa participación internacional. Sobresale además por ser la primera aplicación cuantitativa completa de la metodología ISA, entonces en primera versión, analizando sus detalles matemáticos, incluidos los desarrollos para el tratamiento de las incertidumbre temporales, una de las características diferenciadoras de las herramientas y

métodos integrados.

El presente documento:

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

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

Además de describir y justificar el marco ISA para tratamiento integrado, incluye de manera extensa ampliaciones recientes de los métodos ISA con especial insistencia en el modo de incorporación de los modelos FT/ET del CSN de las plantas españolas y su consistencia con la metodología APS utilizada en todo el mundo, y traza un programa de investigación para su mejora**.**

Algunos proyectos de este programa han sido ya aprobados para su ejecución y otros están en trámite, por lo que esta publicación también se ha pensado como apoyo a la de estos proyectos.

Hacemos notar aspectos redundantes con la información contenida en el capítulo

- "*Why sequence dynamics matters in PSA: Checking consistency of probabilistic and deterministic analyses*"

del libro *"Advanced Concepts in Nuclear Energy Risk Assessment and Management",* publicado por World Scientific Publishing Company Pte. Ltd (2016) ([4]), capítulo elaborado por MOSI, en el que se han extraído y seleccionado los aspectos más relevantes para la comunidad científica internacional dedicada a la optimización de protecciones, independientemente de su aplicación nuclear. Se observará por tanto un acusado acento académico en estos aspectos, algo que se ha considerado importante, ya que este material pretende también ser utilizado, debidamente expuesto en términos didácticos, como base de futuros cursos de formación.

Summary

Summary

History and evolution of quantitative risk assessment methods in the nuclear field are reviewed, and the Integrated Safety Assessment (ISA) unified approach used by the Nuclear Safety Council (CSN) of Spain Modeling and Simulation Area (MOSI) is presented. The purpose of ISA is the independent regulatory verification of the industry quantitative risk assessments. The theory and models behind ISA are summarized, as well as the development of SCAIS (Simulation Codes System for ISA) computer platform and its prototype for testing.

The classical treatment of time in conventional PSA sequences is discussed and important conclusions in order to avoid systematic and unacceptable underestimates of the safety limit exceedance frequencies are stated. The unified ISA method is a feasible procedure that faces this challenge by coupling deterministic and probabilistic mutual influences in scenario evolution. The ISA approach is illustrated with some examples of its applications to full size plants and experimental facilities.

In addition, new ideas to handle the important event timing and uncertainty in boundary conditions are presented to allow dividing/synthesizing the accident progression in smaller problems and to check success criteria in Level 1 probabilistic safety assessment.

List of acronyms

AM: Accident Management

AOT/CT: Allowed Outage Times/Completion Times

APET: Accident Progression Event Tree

SCC: System Component Configuration

DBE: Design Basis Envelope

DBSL/DSSL: Design Barrier/System Safety Limits

DBT/A: Design Basis Transients/Accidents

DDET: Deterministic Dynamic Event Tree

DET: Dynamic Event Tree

EOP: Emergency Operating Procedure

FT: Función de Transmisión (Transmission Function) or Fault Tree

IDPSA: Integrated Deterministic and Probabilistic Safety Assessment

ISA: Integrated Safety Assessment

LCO: Limiting Conditions for Operations

OTS: Operating Technical Specifications

pdf: probability density function

PDS: Plant Damage States

PORV: Power Operated Relief Valve

PSC: Plant System Configuration

RCP: Reactor Coolant Pump

SAG: Severe Accident Guide

SAR: Safety Analysis Report

SBO: Station Blackout

SCAIS: Simulation Code System for Integrated Safety Assessment

SDTPD: Stimulus Driven Theory of Probabilistic Dynamics

SOE/SOT: Sequence of Events/Transitions

TFT: Transmission Function Theory (Teoría de las Funciones de Transmisión)

TPD: Theory of Probabilistic Dynamics

TSD: Theory of Stimulated Dynamics

1. Introduction

1. Introduction

The two traditional approaches to safety analysis in nuclear power plants are the so-called Deterministic Safety Assessment (DSA) and Probabilistic Safety Assessment (PSA). The DSA has been and continues to be the main support for licensing design issues. Plant operation is also constrained by the conclusions of the DSA with respect to automatic protective actions via its Design Basis Transients and Accidents (DBT, DBA) analysis, as reported in the Safety Analysis Reports (SARs). They impose day to day requirements like those included in Operating Technical Specifications (OTS).

Nonetheless, there is an increasing trend to incorporate risk considerations into different licensing issues, and most nuclear safety regulatory bodies make use of PSA models in key aspects of their licensing and oversight activities, including for instance, inspection planning and categorization of their findings, incident analysis, as well as some operational aspects (maintenance rule, human reliability, safety culture, etc.) ([5], [6]).

The overall licensing process encompasses a variety of safety studies, widely different in nature, data, phenomena and systems, each being a piece interacting in several ways with many others. Inevitably, an incremental approach is followed where, in order to face new problems, only new additional studies are performed, rising questions of consistency of the overall approach of risk assessments in actual plants. One important example is the extension of the analysis scope to out of design scenarios to address higher level safety goals after the Three Mile Island (TMI) accident. In these analyses, manual actions and non-safety graded systems are accounted for in order to prevent exceedance of design barrier integrity requirements (which is the scope of the so called Level 1 PSA or PSA1). In addition, other situations where some limits have been exceeded and further barrier degradation is possible, are also considered (Level 2 PSA or PSA2) ([7], [8]).

It is therefore of capital importance to ensure that both DSA and PSA have internal and cross consistency. Ensuring correct risk assessments with their many implicit and explicit assumptions, their interfaces and conclusions, is a major task of the regulatory review. These set of regulatory activities may be considered as a licensing Validation and Verification (V&V) process. Most are qualitative in nature, but the widespread use of computerized analysis also requires sophisticated, quantitative V&V with independent checks complementing the qualitative process ([9], [1]).

Some aspects of the consistency of deterministic and probabilistic studies are involved in the

following issues, that may be taken as representative:

- To which extent and at what stage of the PSA method a significant change in safety systems initiation set-points, with obvious impact in DSA, is reflected in the PSA results.
- To which extent both DSA and PSA cover different operator behaviours, including for instance, time delays in the manual actions.

Together with design related checks, there is also room for improvements in the analysis of operational events and their associated lessons learned, when considering any of the many consistency issues discussed here. Most current approaches to incident analysis focus almost exclusively on safety metrics derived from event tree-fault tree (ET/FT) quantifications, as Core Damage Frequency (CDF), which provide only a partial view of the incident implications.

This publication reviews the history and evolution of quantitative risk assessment methods in the nuclear field and presents the unified approach followed by the Nuclear Safety Council (CSN) of Spain Modeling and Simulation Area (MOSI): the Integrated Safety Assessment (ISA) methodology. The purpose of the development of ISA is the independent regulatory verification of the industry quantitative risk assessments. This review paper summarizes the development of the theory and models behind ISA, as well as the SCAIS (Simulation Codes System for ISA) computer platform and its prototype for testing.

The paper is organized as follows:

- Section 2 reviews the history and evolution of quantitative risk assessment methods in the nuclear field (DSA and PSA), as well as main concepts and techniques used in their applications.
- Section 3 compares the treatment of both dynamic/time and probabilistic aspects of the risk problem in DSA and in PSA, introducing some discussion about where inconsistencies among them may appear. This discussion helps the introduction of the ISA approach presented in Section 4.
- Section 5 describes the main features and elements of the associated computational platform SCAIS and section 6 outlines some of the recent applications of the method and tools for V&V different purposes.
- Section 7 presents the main structure and some applications of the off-line Theory of

Stimulated Dynamics (TSD) prototype, used as a developmental tool for testing ISA/SCAIS improvements. Section 8 discusses the need to find adequate dynamic models for the ISA-TSD method, models able to configure reasonable envelopes for any risk sub-problem. A proposal for the use of surrogate models based on system dynamics piecewise linear approximations, is presented. As emphasized in reference [10], surrogate models become inevitable to handle the infinity of transients involved in the safety envelopes.

- Further research directions are suggested in section 9, and the main conclusions are presented.

2. Main concepts in PSA and DSA

2. Main concepts[1] in PSA and DSA

This section overviews the main and classical concepts underpinning DSA and PSA. Plant systems involved in the regular plant operation are distinguished in section 2.1 from those performing safety related operations, i.e., trip systems and standby safety systems. Section 2.2 deals with barrier and system functions, and conditions for them. Section 2.3 delves into sequences and events, distinguishing events that change the time evolution of plant variables from those not having a direct impact on the plant dynamics.

2.1 Plant and safety systems

To understand safety assessments it is essential in this review to distinguish the plant from its safety systems. By system we mean a set of elementary components (components necessary to perform any of the tasks involved) able to perform the system functions when arranged in adequate configurations. Because the same elements may contribute to different tasks, the component configuration scope of a system ought to be clearly defined and usually includes relations between different tasks that may be modeled with a logic tree. The components may be passive as for instance structures, including piping, or active such as pumps or valves.

Both systems and components may be in several operating modes or conditions (working, shutdown, in standby etc.). Transitions among modes are made possible with other system components (electronic, pneumatic, etc.) or may be the consequence of component failures or operator actions. Together with *system component configurations*, (SCC) we denote by *plant system configuration* (PSC) the sets of systems necessary to fulfil the plant functions.

In the context of this report, a nuclear facility is a set of facility main systems, each being a set of sub-systems that perform operating functions with a production goal in mind. For instance a turbine is a main system constituted by several turbine sub-systems. Also in this context, safety systems are considered as different from the plant systems because they are not intended to contribute to the production goal but to protect the plant itself, the environment, the workers or the public from harmful consequences of abnormal occurrences in the plant. Two groups of safety systems are under consideration: first, trip and standby safety systems (section 2.1.1) and second,

[1] Throughout this review, the USA required safety assessments and its review are taken as the reference ([11], [12]). The Spanish regulation is highly consistent with the USA approach.

those that provide barriers and radiological protection (section 2.1.2).

2.1.1 Trip and standby safety systems

Safety systems will be distinguished from facility systems although they may also share technical elements, the main difference being its purpose which, in the case of safety systems, is to avoid undesired situations. We denote by nuclear plant protection the set of all its safety systems, reserving the term nuclear power plant (NPP) to include both the nuclear facility and the nuclear plant protection.

Safety systems require some initiation signal to actuate. They include trip systems that disconnect some working system from the facility and standby safety systems that get started up and connected to the facility upon the activation signal. Most important trip systems are those related with main facility systems such as the reactor or the turbine. The most typical examples of NPP standby safety systems are the emergency core cooling systems.

Automatic connections/disconnections occur upon initiation signals generated with basically no delay (or with a design specified delay) when a set-point is reached by some process variable or combination thereof. On the contrary, manual connections/disconnections imply a control room/human organization decision process with some undetermined delay between activation of action demand conditions (alarms or operating procedure entry-points) and the effective generation of the initiation signal. More details about connection/disconnection events are given in sections 4.5.4 and 4.6.2, and mentions there.

2.1.2 Barriers and radiological protection

A basic safety strategy of NPP protection is radionuclide confinement via barriers, i.e., specific passive safety systems constituted by successive, enclosed structures including main piping. The barrier safety function, i.e., its confinement capability, requires maintenance of the barrier integrity, characterized by structural indicators that, if not exceeding certain limits (barrier safety limits), guarantee that the barrier function is maintained. Without exceeding these limits, releases of radio-nuclides through barriers are kept below an acceptable maximum that is taken as a basis for the public and environment radiological protection design. NPP protection includes then two important aspects, Barrier Protection and Radiological Protection. This review mostly deals with barrier protection.

Barrier safety functions are hierarchical, i.e., there is a barrier safety function logic, meaning

that higher level barrier safety functions are proved to be successful conditional to the state of certain logical combinations of lower level barrier safety functions. For instance, containment safety functions may be conditional to successful reactor coolant safety functions (see section 2.2.2 and last paragraph of the introduction to section 3.1).

2.2 Safety graded system functions, design barrier safety limits and stimulus activations

2.2.1 Safety system functions and safety graded safety systems

Parallel concepts to those related with safety barriers are defined concerning safety measures. Safety system functions, as its name indicates, refer to the intent of a safety system, as prescribed in its design, very often stated in terms of avoiding exceedance of barrier safety limits.

Safety system functions are also logically related among themselves and with those of other systems, in order to implement basic principles of redundancy and diversity. This implies that several system configurations may be grouped so that their joint configuration satisfies both the safety function and its reliability requirements. We will use the term safety graded systems to denote those with joint configurations that fulfil the qualitative reliability requirements of the design regulations. Thus, they can be credited in the design safety analyses.

2.2.2 Design barrier/system safety variables

Effectiveness of barrier/system safety functions is usually expressed through lower and/or upper threshold limits in process variables. Very often the limits are indicative of degrading phenomena that take place prior to the actual failure of the safety function. As a part of the design strategy, these phenomena may be prevented by avoiding other phenomena necessary for their occurrence, or by encouraging counter-acting phenomena. Such strategy will be convenient if the conditioning phenomena are easier or more convenient to handle, have less uncertainty or are better measured.

For instance, if the reactor coolant keeps sufficient sub-cooling margin, there is little point to worry about two phase degrading phenomena. If DNB (Departure from Nucleate Boiling) limits are not exceeded, cladding burnout phenomena are precluded and if the fuel cladding temperatures do not reach certain limits, cladding oxidation will be limited. In the safety system side, a protective action like

supply of sufficient injection flow may be enough to guarantee protective cooling. As seen in the examples, the process variables involved in the different strategy formulations may be very different. The regulations fix the required barrier limits and minimum requirements for safety graded system functions to protect the barriers, but designers may also use more convenient ones, that we call Design Barrier/System Safety Limits (DBSL/DSSL), provided they are not less restrictive.

The protective phenomena may also be induced intrinsically when the process variables enter certain regions without active systems involved, which is at the basis of the so called intrinsic or passive safety. For instance a certain geometry design may induce natural convection phenomena without any need of external actions. A most classical example is, of course, the Doppler effect that induces negative reactivity. NPP protection includes then intrinsic as well as external protections.

2.2.3 Stimulus activations and safety variables

In general we call stimulus activation the set of conditions that make possible the ocurrence of some phenomenon or the call for an active safety measure. Again, these conditions usually adopt the format of exceeding process variable thresholds, although they may be combined with other features, like the state of the plant systems. Examples are set-points, alarms and procedures entry points for external protection, the onset conditions for protective phenomena in intrinsic protection or the conditions for occurrence of some stochastic degrading phenomenon. The term *safety variable* will denote any process variable used to formulate stimuli or barrier safety limits or to define safety system functions, usually in terms of interface variables between the safety system and the plant.

2.3 Sequences of events, and dynamic event trees. Relations with ET/FT

An event may be considered a probabilistic concept, indicating stochastic occurrences, i.e., that something may or may not occur among a given set of possibilities (probabilistic space). Deterministic events in this context are limiting cases. The probabilistic space may take many different forms, for example the set of transients in a plant that belong to a given group (transient probabilistic space). The importance of events in quantitative safety assessments is related to the efficiency of the safety measures taken, because they may induce phenomena able to change the time evolution of the process variables (dynamic transitions), preventing them (or not) to enter unsafe regions. This requires distinguishing dynamic events, i.e., those inducing dynamic transitions of the process variables, from static events not doing so.

A Sequence of Events (SOE) is an ordered set of events. If only dynamic events occurring in a transient probabilistic space are taken into account, the sequence is called a *dynamic sequence*, although it may also contain static events. The first event (initiating event) is assumed random[2] and starting from a safe (i.e. satisfying safety requirements), initial steady state. The rest of the dynamic events are conditioned by stimuli, stimulus activations being a particular type of static events. The end of the transient is either a steady state with all the safety variables within the ranges delimited by a specified subset of DBSL or the exceedance of some of those specified DBSL. A Dynamic Event Tree, DET, collects all SOE with the same initiator and the same specified subset of DBSL. The dynamic events common to several sequences of the same tree are called headers of the DET.

These definitions are easily extended to other probabilistic spaces. In addition to transient probabilistic spaces, most relevant ones are the set of tasks (including system component functions) necessary to meet a system function. Failure-of-task events may be defined there, which allows to compute system function failure probabilities (via for instance a Fault Tree).

To emphasize the case of dynamic events, the notation DET (Dynamic Event Tree) will be used. The relationship between ET/FT and DET is further discussed in section 4.6.3.

[2] If not, they are supposed to belong to other sequences.

3. DSA versus PSA

3. DSA versus PSA

Despite the usual terminology, both DSA and PSA involve deterministic and probabilistic aspects. Differences are in the scope and the objective of the analysis and in the relative weight and level of detail of the analysis methods. DSA is mainly oriented to assess the effectiveness of automatic safety systems under the assumptions of their design basis, while PSA tries to evaluate overall plant safety taking into account the likelihood of possible interactions of these systems with the ongoing processes, as well as human intervention. An important feature of automatic versus manual protective actions is that, in the first case, both dynamic events and activation events occur almost simultaneously (with negligible or design-specified delays) while, in the second, significant and uncertain time delays may exist between stimulus activations and their associated dynamic events.

This section focuses in the treatment of both aspects of the risk problem in DSA (section 3.1) and PSA1 (section 3.2) approaches to safety assessment. They give rise to the majority of licensing and operational concepts, such as Design Basis Transients and Accidents, Operating Technical Specifications, or Success Criteria. The framework may also be used in PSA2 although it requires paying further attention to the uncertainty of processes and phenomena (see section 3.3).

3.1 DSA

The term DSA historically refers to the analysis of Sequences of Transitions (SOT) (see below) resulting from sequences of deterministic dynamic events, in the domain of transients satisfying certain features matching the assumptions of the design basis for automatic safety systems. Note that a transient[3] is a deterministic time evolution of the safety variables involved in the events as a consequence of the dynamic transitions (SOT) of a Sequence of Events (SOE). Best Estimate (BE) codes are deterministic, so they can only simulate single transients. The DSA analysis space (i.e., the automatic design space) is restricted to transients with almost no time delay between demand and initiation of safety actions and with specified (by fairly prescriptive regulations) configurations of safety graded systems which include some postulated failures.

The DSA analysis space is subdivided in classes (for instance, ANSI-N-18.2 condition I, II, III and IV), with more or less restrictive class requirements depending on a qualitative estimate of

[3] Also denoted *transient paths* or *paths*, because they may be associated with trajectories.

frequencies (see section 4.6.2). Since probabilities are embedded qualitatively through safety graded configurations, DSA consists basically on the analysis of a set of Design Basis Transients and Accidents (DBT, DBA) for each class. Those are *distorted scenarios* both in models and assumptions that all together are supposed to envelope all actual scenarios within the automatic design transient space. That means that probabilities are not computed (see below), so the DSA transient analysis space is not a probabilistic space but an envelope space[4]. The set of DBT/A is usually referred to as the Design Basis Envelope (DBE). See section 4.4 for a better description of envelopes.

The main regulatory design criteria (as referred in ref. [11]) try to ensure that all the safety variables for all SOT, consequence of sequences of deterministic dynamic events, are within the barrier safety limits specified for the corresponding class of the automatic design space. For instance, for initiating events that may occur once in the life of the plant, only a single failure of the active safety systems is assumed (other than the initiating event) and the fuel barrier integrity is required to satisfy the so called "specified acceptable fuel design limits" to be approved for each fuel design. Given those, coolant and containment barrier criteria are also prescribed for this class. The same occurs for other classes within the DBE.

3.1.1 Quantitative versus qualitative, probabilistic aspects in DSA. The importance of system component configurations

Prior to the TMI accident, DSA was the realm of the safety analysis. The most important products were to determine the stimuli for automatic safety measures (Limiting Safety System Settings or LSSS) as well as its associated Limiting Conditions for Operations (LCO) or initial conditions of the transients, and to establish design barrier safety limits as well as safety graded system safety functions. All together they constrain the operation of the plant (i.e., they define the OTS), and are strongly dependent on the design choice of safety limits.

It was also necessary to define the times allowed for a safety system to be out of service (i.e., Completion Times (CT), formerly called Allowed Outage Times (AOT), which were traditionally decided upon using qualitative arguments. Because of its importance, the CT issue prompted more detailed studies incorporating system reliability techniques that were maturing in parallel, so as to make quantitative and precise statements about safety systems availability and reliability expected to be

[4] However, within the context of ISA (see section 4) we will as well consider it as a transient probabilistic space.

equivalent to the qualitative requirements of safety graded systems.

3.1.2 Incorporation of system reliability techniques in safety graded systems

To better understand the approach followed, an active system function, that may be defined in terms of keeping the system process variables within specified regions, may also be represented in terms of several alternate component configurations (SCC, i.e., combination of success and failed component/operational tasks), each configuration able (not) to meet the system function. To quantify SCC probability, component events (as opposed to dynamic events in system configurations) are understood as task events, with no reference to process variables, rather as empirical facts that may be verified and statistically quantified.

System Reliability techniques, as for instance fault trees, exploit the internal structure of the systems by associating a logic tree that correlates failures of system configurations (high level, multi tasks) with basic tasks failures (basic events), that may be considered independent. Using Boolean techniques to characterize the logic, very complex configurations involving high number of basic events may be handled, so it is possible to compute their probability.

Note that in this representation events are not dynamic, and the only time dependence of a Fault Tree is due to the evolution in time of the configurations themselves. A sequence of events and ET/FT may also be defined, but the probabilistic space is a task space. Note also that component configurations of different systems may involve common elements, particularly in view of the fact that certain important system requirements like electric supply are shared (support systems).

As well known, the essence of the fault tree and similar techniques (e.g., Binary Decision Diagrams, BDD) is to solve this important issue, that is, to find the failure probabilities accounting for so many dependencies. Boolean events, elements of a Boolean space, are used to describe the component dependent failure rates associated to the different component configurations and to reduce the problem to a set of failure rates of independent components (basic events). If those components turn out not to be independent, additional “gross” techniques are used (i.e., the “common cause events” problem).

System success criteria select the set of system configurations that end-up in system success. Thus, the probability of success is linked to that of the success configuration set.

3.1.3 Operable states of standby safety systems

The reason to introduce system component configurations in the CT problem of the DSA is to be able to use the power of system reliability techniques, among which the most popular is the FT/ET technology, in order to make a quantitative approach to the previously qualitative estimates of the CTs.

The method profits from the fact that active stand-by safety systems are all plant interface systems with environment, so it is possible to divide the DSA problem into two (a particular case of problem division, see sections 3.3.3 and 4.5.4):

1. A first one where the safety system in the plant model is represented by including in its safety variables the system function as input boundary conditions on common system and plant process variables characterizing the functions (for instance cooling flow). The DSSL are imposed on the plant model as additional constraints in these inputs, adding them to the DBSL and stimuli as safety variables.
2. A separate problem where the boundary conditions are environmental parameters and the DSSL play the role of DBSL in problem 1. The safety system model may now be very detailed, and the operating configurations associated with the system success are confirmed through a separate system analysis.

   This separate analysis aims to demonstrate that if

   - the system initial state is in any steady stand-by configuration (*operable state* as defined in the OTS), and considering
   - the sequence of component configuration changes (involved in starting the system manually and/or automatically), required to bring it to any of the success configurations,

it can be verified that there is no violation of the DSSL. This is the crucial point that links reliability techniques with dynamic transient accident analysis and will be touched again in section 4.6 below and extensively in ref. [2].

This separate problem has now the same set-up as the plant problem in point 1 above, so the same approach can be used in both. It can be considered as the deterministic DSA analysis of the separate safety systems, as reported in the SAR of the plants.

3.2 PSA

As part of the many lessons learned after the occurrence of TMI, two very important issues came under focus:

- It was necessary to pay more attention to the design of manual protective measures, i.e., the set of operating procedures, which implied extensions of the transient envelopes and safety graded system configurations (DSA spaces) in several aspects:
  - to consider out of design safety system configurations beyond the safety graded ones, including multiple failures;
  - to release the assumption of no delays, and
  - to establish a more detailed approach to regulate the design of operating procedures with special attention to Emergency Operating Procedures (EOP).
- It was necessary to consider core melt scenarios and their consequential, beyond design, barrier source terms.

3.2.1 PSA1: Success criteria and safety targets

The aim of a PSA1 study is to perform a risk assessment of out of design situations that may challenge the same required barrier safety limits of the DSA, but accounting for non-safety graded systems together with operator actions and allowing multiple failures. Design barrier safety limits then become *sequence success criteria*, since they distinguish when the set of safety measures, all together, succeed or fail in limiting the effects of an accident. It is not a question of new design requirements, but to estimate the risks of the design.

The main figure of merit is the frequency of exceedance of the sequence success criteria in the set of PSA sequences, i.e., the frequency with which the design would exceed the barrier safety limits when accounting for the new situations. Some limits on the exceedance frequency (safety targets) are considered to guide the regulatory and EOP design implications, far less prescriptive than safety limits in the design case.

An envelope SOT barrier analysis, similar to that of DSA but using different assumptions and restrictions, allows identifying the PSC subset of safety systems that satisfies the sequence success criteria. Thus, PSA1 system success criteria are different than in DSA as further clarified below.

In the same way, SCC associated to system success criteria are established by a process similar

to the one described in point 2 of section 3.1.3, again different now than in the DSA case (see section 3.2.3).

3.2.2 PSA1 method and guides

The PSA1 method is well defined in several sources, i.e., PSA guides (see [13], [7], [8] and chapter 19.0 of [12]), that establish three main stages in a PSA1 study, namely:

1. Delineate the possible SOE resulting from initiating events followed by a sequence of protective actions as well as possible failures of safety systems.
2. Determine system success criteria and available times for operator actions.
3. Identify failed sequences (i.e., those where the sequence success criteria have been exceeded) and compute the frequency of each one by using, for instance, FT/ET techniques. An additional challenge is how to consider operator actions in the reliability calculations. This requires incorporating the field of Human Reliability Assessments (HRA). Again consistency issues arise.

While detailed methods and abundant literature ([7], [8]) provide guidance for Stage 3, such a guidance become loose when describing Stages 1 and 2, mainly due to the unique phenomena involved in each application domain, their strong nonlinearities, and their dependence on the protection design methods, usually very sophisticated and technology dependent as described in Safety Analysis Reports (SAR) ([11]). This is perhaps the most complex issue to tackle in consistency verification of PSA1 (see section 6.2.2).

3.2.3 Handling time in DSA+PSA1

In DSA, time is essential although the DBT envelope approach obscures how to interpret it. Indeed, DBTs being distorted transients, their dynamic analysis does not provide clues on real times. However, to verify their envelope condition (the umbrella condition) within each DSA transient class requires to deal with real transients one way or another. Thus, design verification requires event timing to be handled, so any diagnostic method will require it.

On the other hand, PSA1 rules do not consider time explicitly. However, this is more apparent than real. To start with, it is evident that a successful safety measure, if delayed to a certain delay value becomes unsuccessful in at least some transient of some sequence; otherwise there is no point to

keep it as a header of the ET. This means that the maximum time elapsed since the measure is decided 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 DSA zero delay assumption.

Because automatic actions correspond to almost zero delays, the PSA system success configurations are the DSA safety graded configurations enlarged with those satisfying the same DSA system performance requirements but including the additional systems used in the procedures, perhaps non-safety graded. A main issue in this extension is the determination of the associated available times and how to ensure them in the operating actions of the procedures including post reactor trip situations (i.e., EOP). To facilitate their design, a set of specific design barrier safety functions (Critical Safety Functions or CSF) are introduced (ensure sub-criticality, heat removal, etc.) with associated safety system configurations.

Finally, there are other considerations that show the need for paying more attention to time in PSA1. The transition rates of the DET are actually dependent on the process variables. Of particular importance is the impact of stimuli which is always present in the DET side. Indeed, the transition rate associated with a successful header is zero unless its stimulus is activated, which, as indicated, implies a strong dependence on process variables.

In the same way, the rates of component failures may also be dependent on process variables. For instance, the rate of failure of a valve may depend on its temperature. In addition, house events that represent the Boolean boundary conditions of the FT, often end-up in a sequence stimulus activation or other type of dependence on process variables.

From the above, we may consider DSA/PSA, DET sequences as those including both stimulus activations and dynamic transitions. This is the main feature of the ISA sequences (see section 4).

3.3 Extension to other PSA accident progression stages

Previous sections have clarified concepts, jargon, purpose and problem setup, as they developed historically and extended to include out of design situations, under the scope of barrier integrity analyses. However, after the TMI core melted, it was also necessary to account for barrier degradations outside the design limits, including for instance vessel failures.

That means that another extension of the out of design world was due, this time involving

new phenomena and new menaces to the barriers ("beyond design" situations). The nature of the radionuclides and composition of source terms escaping from more degraded barriers also changes drastically with respect to the design sources.

The occurrence of the Fukushima accident has made even more inevitable to take care of this. The beyond design world is however a very low frequency sequence domain (it has been termed the residual risk domain). The phenomena are often not enough known (i.e., large epistemic uncertainty that is much smaller for the design envelope), so from the point of view of SOE we will need to account for stochastic phenomena and their uncertainty; again, a new enlargement of the probability space. Since PSA1 may be considered as the first progression phase prior to core damage, PSA2 extending the methodology to other progression phases, we will devote the next sections to detail this view.

3.3.1 Vulnerability and accident management analysis

The PSA2 problem has two main aspects that lead to the so called "vulnerability analysis" ([14], [15], and chapter 19.0 of [12]), where no additional safety measures are taken and "accident management (AM) analysis" when the measures are included. The first was developed by using the best existing knowledge to identify safety variables and safety limits related with severe barrier degradation mechanisms and their associated source terms, looking for those combinations leading to higher exceedance frequencies. The second estimates the efficiency of protective measures by including accident management (AM) strategies to be tried from Technical Support Centers providing guidance to the control room crew.

3.3.2 Deploying the accident progression

From a modelling viewpoint, the setup of the vulnerability analysis may be made with the help of one of the so-called integrated codes, able to describe most phenomena and the system impact on the dynamic evolution of damage indicators throughout the accident progression.

A block diagram, where each block is a meaningful subset of the code equations, may be used to describe the interactions involved in damage variable evolution. Arrows in the block diagram represent time dependent boundary condition variables exchanged by the blocks. Many feedback effects among the blocks are expected, but only a handful of overall boundary conditions are necessary to trigger the simulation of the consequences of the initiating event.

The essence of the block diagram is to show the completeness of the input-output, and to visually describe feedback and feed-forward relationships. It can be developed to different levels of detail but to describe the overall PSA2 problem a high level (low detail) block diagram may suffice. Figure 1 shows the block diagram corresponding to the MELCOR code ([16]), including as block names the associated code packages.

Note that several codes may have dissimilar high level blocks, but for a given code, the blocks are basically unique, providing an unambiguous description of the structure of the dynamics of systems and phenomena considered during a progression interval. It is also possible to include in the diagram some blocks representing specialized codes, for instance codes modelling shock phenomena, interacting with the overall model. Block diagram structuring may be aided by modern computer technology, generating a traceable engineering process.

Associated with block diagrams and/or part of them, the stochastic events may be represented by switches within the diagram associated to whether or not the phenomena (or systems actions) take place, fail or are not activated. This way, all the ET header candidates may be explicitly identified. Activated stimuli (i.e., set points or alarm conditions), are associated to the switches as necessary conditions for their actuation, so the sequence of events actually include activations as well as dynamic events. However, it is difficult to ascertain without simulation the activation conditions and the development of sequences. With the stimulus activated, the system or phenomenon represented by the header may or may not come into play, modifying or not the block diagram model and consequently its dynamic evolution.

Once the block diagram that links the output damage variable to the initiators and headers is defined, as well as the switches associated to the events, we consider that a PSA2 problem is well posed if probabilistic models to estimate the associated exceedance frequency for each block output of interest are available. The estimates may be made more or less detailed, reflecting the level of knowledge (e.g., expert judgment, operational or accident data, fault trees; see section 4.6.4) and very often they are limited to a qualitative classification with a rough number associated.

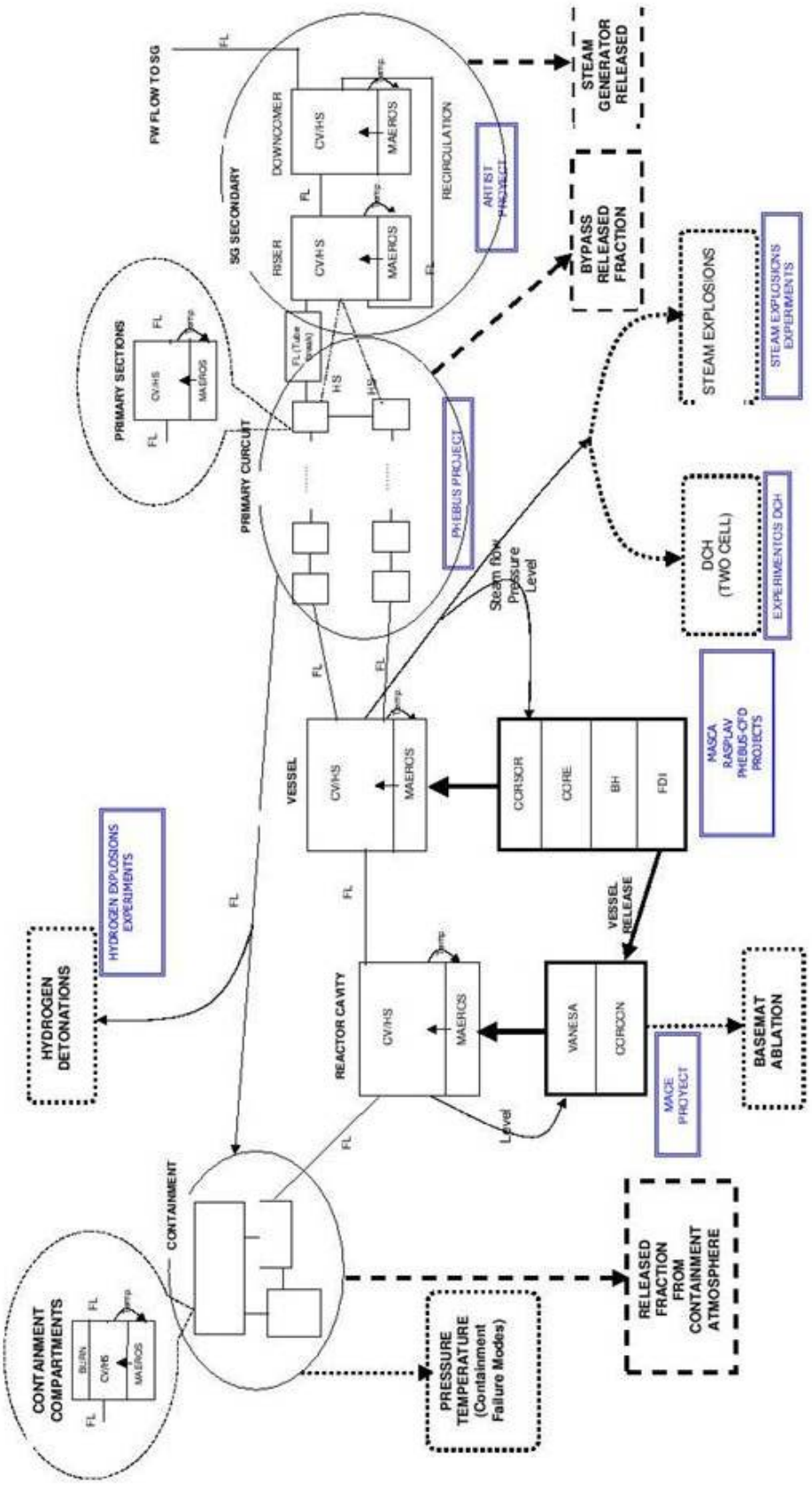

Figure 1. Block diagram of processes and phenomena considered in the MELCOR code.

3.3.3 Division in sub-problems

Usually the whole PSA2 problem is divided into smaller sub-problems, each of them equally well posed, by using several techniques that depend on whether we are dealing with a vulnerability or an AM problem and on the nature of the progression interval.

Let us describe the main features of the vulnerability analysis of a PSA2. The calculation of the exceedance frequency of undesired situations and its uncertainty band is the main focus in this case. Usual techniques are:

1. sub-problems associated with accident progression phases (e.g., very early,early, late or very late), defined by the activation of different phenomenom stimuli. Each phase generates precursor sequences for the next; in particular PSA1 sequences are precursors for PSA2, so PSA1 may be considered as the first phase.
2. sub-problems associated with necessary conditions for source terms. For instance different modes of vessel and containment ruptures give rise to different pathways for releases.
3. sub-problems associated with loosely coupled plant system sets, like containment, reactor vessel and its cavity, the primary reactor coolant and the balance of plant systems. Boundary conditions coupling these plant subsets, particularly the core and reactor cavity, ought to be addressed.

Each sub-problem for the different phases, failure modes and plant areas is characterized by attributes[5] that then classify and group partial ETs involving both system and phenomena related events. Common attributes couple the sub-problems and allow synthesizing an overall system/phenomena Accident Progression Event Tree (APET) ([14], [17]).

The system portion of the APET is handled with usual Boolean techniques like ET/FT assuming PSA1 safety system limits and success criteria (first progression phase) and their cut sets grouped by system attributes (i.e., Plant Damage States, PDS). For each PDS, the APET sub-sequences are then grouped again by phenomenological attributes and quantified. The resulting probabilities along with PDS frequencies and the estimation of the magnitude of the source term as a function of the sequence attributes finally provide the exceedance frequency curves with uncertainty bands.

[5] Attributes are labels of a wide variety, mostly referring to the state of the systems, nature of phenomena, the level of the progression and the subsystem being analyzed. They may be common to several sub-problems.

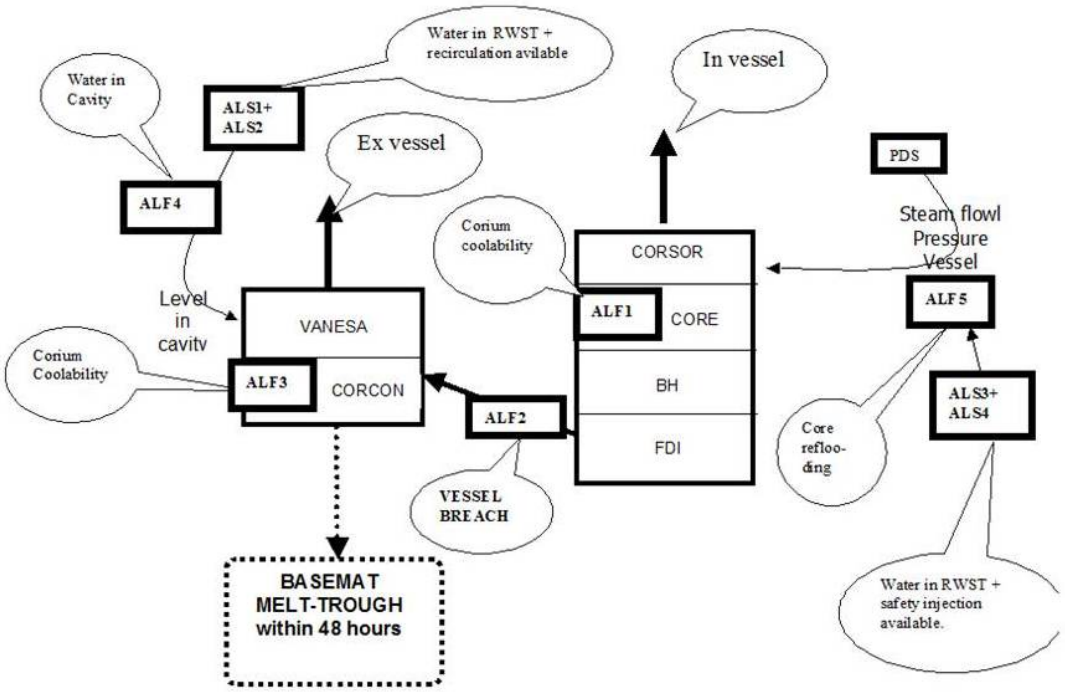

Figure 2. Block diagram and headers for basemat melt-through containment failure mode.

An example of a loosely coupled plant system set of the MELCOR block diagram and headers is the basemat melt-through failure mode sub-problem as shown in Fig. 2, which details the blocks representing in-vessel and ex-vessel phenomenology in Fig. 1. The basemat melt-through output and the in-vessel inputs associated respectively with the code elements CORCON and CORE in Fig. 2 constitute the quantification set-up of the basemat melt-through problem.

As for the time variable, a similar approach is followed by subdividing the problem according to the time scales of phenomena and system configurations, resulting in the so-called the binning process (see sections 4.5.2 point i and 6.1).

4. Integrated Safety Assessment (ISA) and Barrier Protection verification

4. Integrated Safety Assessment (ISA) and Barrier Protection verification

This section presents the Integrated Safety Assessment (ISA) and its relation with the verification of Barrier Protection. Section 4.1 introduces the scope of ISA and its associated computational platform SCAIS (Simulation Code System for ISA), the main problem it tries to solve as well as the limitations of the method, and section 4.2 justifies the use of envelope techniques. Section 4.3 summarizes the chronology of the ISA-SCAIS development. Section 4.4 details the successive steps followed for ISA application, whereas TSD equations for computing the frequency of exceeding some damage conditions are introduced in sections 4.5 and 4.6.

4.1 Scope and limitations

The main purpose of this review is to show a unified methodology (ISA) and a computer platform (SCAIS) ([1], [2]), to verify that protection design and operation fulfill their intended purpose, meeting regulatory requirements, through a set of independent analytical checks made with appropriate computer codes and methods. It covers verification of DSA, PSA1 and PSA2 assessments with special emphasis in the consistency of the deterministic and probabilistic analysis in actual plant risk assessments. ISA/SCAIS is an attempt to formulate/compute a mathematically precise and unified quantitative safety assessment approach, although of limited scope.

Within its scope of application, the main problem in PSA and ISA is to decompose the overall risk assessment in sub-problems linked among themselves both through the consequences of the accident progression and their relative frequency contribution. The most complex aspect is that, in order to account for the consequences, we need to perform simulations using adequate deterministic dynamic models, but accounting for frequencies requires consideration of too many of those simulations.

Advantage can be taken from the fact that we only need to envelope the evolutions to ensure that the relevant safety variables do not exceed required limits, i.e., sufficient margins are available ([3]). However, large margins are often precluded, since safety measures associated to the underlying design are aggressive and there is a principle to intervene when necessary but not if unnecessary. Note the great difference between enveloping and taking representative samples of the scenarios, as further clarified in section 4.2 below.

Then the approach needs to handle the envelope issue in any sub-problem, with a unified method that may be applied irrespective of the type of phenomena and systems. Actually, due to the wide range of time scales and phenomena in the different progression phases (from fractions of seconds in phenomena related to neutron chain reaction excursions and shock phenomena like explosions, to months in those related to cooling melted cores), the trend towards unification is already embedded in the nuclear industry risk assessments.

Indeed, the already consolidated system reliability techniques in use today are an example of this trend, and ET/FT computer codes and technology use the same math software in a wide variety of application domains. However, to guarantee the consistency between the treatment of dynamic aspects of the time evolutions and the associated frequency computation, which is the heart of the ISA contribution, will also require unified methods in the transient simulation side.

In general, the envelope problem rests on ensuring that all the possible SOT, consequences of the SOE that may be involved in the accident progression, have been identified and that analysis cases cover, for each sequence, uncertainty in initial conditions and key data, as well as, most important, boundary conditions and protective action timing. These uncertainties easily explode the number of situations to consider, so that brute force techniques based on reproducing transients with best estimate simulations usually fail in the completeness of the situations considered to demonstrate the (umbrella) envelope character of the analysis. Refer to sections 7 and 8 for more details.

One important limitation, unfortunately present in several applications of interest (fires, electric power networks for instance) is how to deal with too many initiators. Fires or electric faults for instance may arise in many places/electric lines of a plant/network. The techniques described here assume a finite number of possible initiators. When this is not so, they are applicable once the problem has been reduced to a finite group by characterizing them first. Often however, it is this reduction the heart of the analysis. Other limitations are stated in section 4.6.4.

4.2 Aggregating APET risk sub-problems

Figure 3 deploys the strategy commonly followed to ensure that all relevant situations are covered, including the division in sub-problems as means to account for the accident progression

(APET) in the vulnerability analysis ([9], [17]). In the case of barrier protection sub-problems[6] the ISA approach makes use of the Theory of Stimulated Dynamics (TSD) probabilistic model (see section 4.4) to provide a more rigorous estimate of the APET conditional probabilities.

For instance, boundary conditions representing the impact of neighboring areas are time dependent functions that are computed at different phases of the accident progression. Outputs from each sub-problem are inputs to other ones in a block diagram (see section 3.3.3) with initial conditions computed at the end of the prior progression phase.

The method uses adequate models to simulate the transients, that is, models able to envelop the group of transients of each sub-problem. The ISA approach then shows how to compute the probability of each sub-problem output process variable conditioned to the APET restrictions, including those of their process variable inputs (see section 4.6.4). This way, a more rigorous computation of the APET input data is made. Traditional PSA2 computer software may then be used to compute the overall PSA2 exceedance frequency ([17], [2]).

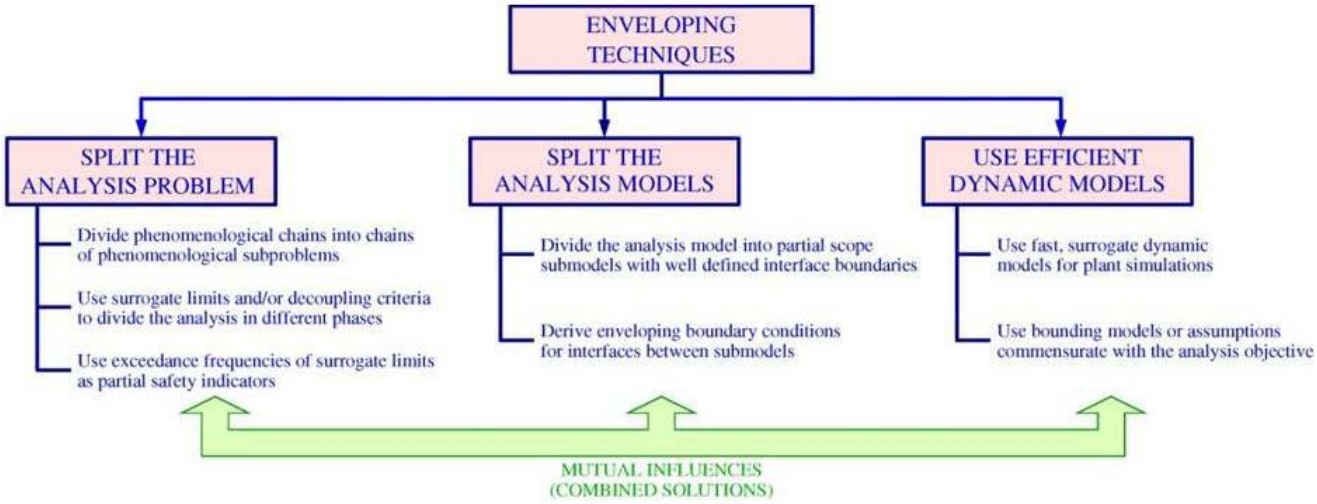

Figure 3. Strategy to ensure that all safety relevant situations are covered.

[6] We do not deal with the PSA2 treatment of source terms, but the classical PSA2 method may also be refined with the TFT modules (see section 9.1.2).

4.3 ISA development

ISA is the result of several prior developments that basically followed the need to enlarge V&V capabilities paralleling the evolution from DSA to PSA1 and PSA2. Figure 4 summarizes this process.

Initially, ISA proposal followed the so called Deterministic Dynamic Event Tree (DDET) approach, also used by other international groups ([18], [19]). The purpose was twofold:

1. To make an automatic delineation of sequences in DETs, ensuring that stimuli were indeed activated (see section 4.6.3 for the importance of this).
2. To be able to verify the efficiency of procedures via models able to simulate their execution without failures, i.e., automatic pilot simulations.

Concerning frequency, Markov techniques were also popular as an alternate to ET/FT where the main ingredients are the transition rates between dynamic states (see section 4.5). Estimates of these rates at the DET branching points allowed to incorporate probabilities as the DET was developed (DDET approach, see section 5).

At the time, several other methods were devised like the Cell to Cell Mapping Technique (CCMT) ([18], [19]) and the Theory of Probabilistic Dynamics (TPD) ([20], [21]). TPD was able to cover both types (DDET and CCMT) of existing methods in a unified approach ([18], [19]), so it was the appropriate choice.

However, TPD did not incorporate the important issue of stimulus activation events ([22]). Its extension was baptized as the Stimulus Driven Theory of Probabilistic Dynamics (SDTPD) ([23], [24], [25]). It is a general solution but at the same time difficult to implement in the engineering arena, where so much work was already done on ET/FT models for PSA and dynamic plant models for DSA.

From the verification perspective, it is indeed a must that any new development 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, [26], [27], [28]) 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, being fully compatible with current PSA models and techniques.

TSD is the theoretical basis for the probabilistic aspects of the Integrated Safety Assessment method (ISA) that is implemented in SCAIS (Simulation Code System for Integrated Safety Assessment) computational platform described in section 5 below.

Additional developments, aimed at efficiently incorporating the uncertainties in event timing and boundary conditions (see section 8), led to the development of the Transmission Functions Theory (TFT) ([30], [31]). Consideration of these uncertainties is required for the assessment of success criteria in PSA1 and for the computation of inputs to APET in its extension to PSA2.

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	• Extension 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. [9], [18], [33], [34], [35], [36], [37], [38], [39], [40]	Ref. [22]	Ref. [23], [24], [25]	Ref. [22], [26], [27], [28], [29], [30], [31], [32]

Figure 4. Development of the theoretical framework for ISA.

4.4 ISA-TSD methodology

The purpose of the analysis of sequences of events in PSA was reformulated in ISA in terms of transients in the following way: compute the exceedance frequency of safety variables associated to the design barrier safety limits under consideration. That is, the main outcome of ISA is the frequency with which the transients in the sequence violate their design barrier safety limits (sequence failure) conditioned to the initiating event occurring from the specified initial state and to that:

1. the system safety variables remain within or out their limits (their DSSL limits) for successful or failed system headers, respectively,
2. the stochastic phenomena take place (or fail) for phenomena headers, and,
3. the stimulus variables (for systems and phenomena) reach their activation limits in case that the corresponding header is taken into account, either in successful or failed state (see section 4.5.3).

The method assumes that best estimate codes are available to deploy the accident progression playing the role of the MELCOR code in the example of section 3.3.

4.4.1 Probabilistic Space and uncertainties in ISA

The probabilistic space is the set of possible transients in the transient envelope space involved in the assessment problem (DSA, PSA1 or any sub-problem of the PSA2, Fig. 1 and 3) under study (see section 4.1). It includes transients accounting for all uncertainties, namely:

1. Initial conditions
2. Uncertain data (parameter uncertainty)
3. Event timing
4. Boundary conditions

compatible with the probability space under check (DSA, PSA1, or a PSA2 sub-problem).

The essence is to find methods to compute the contribution to the exceedance frequency of each transient in the envelope space, in such a way that the sequence frequency is the aggregate of them. The ISA differences of DSA versus PSA1 or PSA2 sub-problems lies, leaving aside the different purpose and scope, in the envelope space definition and applicable safety limits, but the method is unified, the setup of each problem having the same mathematical structure.

4.4.2 Sequence envelopes and failure domains

The ISA-TSD method then lowers the assessment of any sub-problem from the system configuration sequence level, to the transient level within each sequence, by:

1. Considering dynamic sequences as large groups of transients, resulting from dynamic and activation events associated to a random initiator and a design barrier safety limit. (sequence envelopes)
2. Simulating a number of those 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 ought to be simulated depends on the desired accuracy of the failure domain characterization but, in general, this number is very high.
3. Using TSD algorithms to compute the contribution to the exceedance frequency of any transient that belong to the sequence failure domain, then aggregating these contributions for all the transients there.

Included as factors in these algorithms (see section 4.6.2.1 and Fig. 5) are ET/FT results in per-demand terms, as well as the failure probability of activating the stimuli (the demand of active safety measures, or the onset of phenomena) and the probability of failure of operator actions (see Eq. (4.14)).

4.5 The path and sequence approach

TSD may be seen as an extension of the more common Markov and semi-Markov approaches for modeling systems with discrete states and time and process variable dependencies.

4.5.1 The semi-Markov path and sequence solution

The differential semi-Markov equations for the probability $\pi_j(t)$ of being in state *j* at time *t* can be applied to systems whose states may change in a stochastic way as a result of transitions induced by events. Those events occur with occurrence rates $p^e_{j\to k}(t)$ where index e identifies the event at time t and $j\to k$ is the resulting transition. In semi-Markov systems these transition rates are allowed to be a function of time, which allows considering many more situations than in the case of constant rates. As it is well known these equations take the form of a typical probability balance, involving the frequency $\varphi_j(t)$ of entering state *j* at time *t* (ingoing density), and the probability $\pi_j(t)$ of being in state *j* at time *t* as follows

$$\frac{d}{dt}\pi_j(t) = -\pi_j(t)\sum_{k\neq j} p^e_{j\to k}(t) + \varphi_j(t)$$
$$\varphi_j(t) = \sum_{k\neq j} p^e_{k\to j}(t)\,\pi_k(t) \qquad (4.1)$$

The solution can be written in terms of integral equations for $\varphi_j(t)$ and $\pi_j(t)$ as follows

$$\varphi_j(t) = \int_0^t d\tau \sum_{k\neq j} q_{jk}(t,\tau)\left[\pi_k(\tau)\delta(\tau) + \varphi_k(\tau)\right]$$
$$\pi_j(t) = \int_0^t d\tau \left[\pi_j(\tau)\delta(\tau) + \varphi_j(\tau)\right] e^{-\int_\tau^t ds \sum_{k\neq j} p^e_{j\to k}(s)} \qquad (4.2)$$

In these equations, δ stands for Dirac's function and $q_{jk}(t,\tau)$ is the probability density of entering state *j* from state *k* at time *t*, after remaining in state *k* from τ to *t*. It is given by

$$q_{jk}(t,\tau) \equiv p^e_{k\to j}(t)A_k(t,\tau) \quad A_k(t,\tau) \equiv e^{-\int_\tau^t ds \sum_{l\neq j} p^e_{k\to l}(s)}$$
$$\sum_{l\neq j} q_{lk}(t,\tau) \equiv \sum_{l\neq j} p^e_{k\to l}(t)A_k(t,\tau) = -\frac{\partial}{\partial t}A_k(t,\tau) \quad any\ \tau, t$$
$$\sum_{l\neq j} \int_\tau^t q_{lk}(\tau,u)du = A_k(\tau,\tau) - A_k(t,\tau) = 1 - A_k(t,\tau) = U_k(t,\tau) \qquad (4.3)$$

When the problem is formulated with known $p^e_{k\to j}(t)$, Eq. (4.3) satisfies all requirements. However, not any set *j,k* of functions of the two variables τ, t is a valid $q_{jk}(\tau,t)$. Among others, the set should satisfy the additional properties included in Eq. (4.3).

Equations (4.2) account for the contribution of all the possible states to the probability of each state as a function of time. A solution results from the consideration of every possible transient trajectory from the initial state j_1 at τ_1 to the final state j_n at t, which will be called a *path*, composed by a set of *n* transitions caused by dynamic events $e_1, e_2, .., e_n$. The ordered set of such events is called a *sequence*, represented by $\vec{e}_n$ and a sequence ending in state j_n will be represented by $\vec{e}_j$. The initial conditions of the system are given by the frequency $\varphi^{in}_{j_1}(\tau_1)$ of entering state j_1 at $t=\tau_1$, the time of the first event. This solution allows rewriting $\varphi_j(t)$ as

$$\varphi_{j_n}(t) = \sum_{j_1} \varphi^{in}_{j_1}(\tau_1) \sum_{\forall \vec{e}_j \neq e_1} \int_{V^{n-1,\vec{e}}_{\vec{\tau}_{n-1}<t}} d\vec{\tau}_{n-} Q^{\vec{e}_j}_{j_n,j_1}(t \mid \vec{\tau}_{n-1}) \tag{4.4}$$

Summations in Eq. (4.4) extend to all the possible sequences entering state j_n at time *t*. Each sequence starts from an initial state, goes through intermediate states $j_1, j_2, .., j_{n-1}$ and ends in state j_n. Vector $\vec{\tau}_{n-1} \equiv (\tau_1, \tau_2, .., \tau_{n-1})$ represents the occurrence times of events $e_1, e_2, .., e_{n-1}$ and the final event e_n occurs at time *t*. The space of all the $\vec{\tau}_{n-1}$ vectors such that $0 < \tau_1 < .. < \tau_{n-1}$ is represented by $V^{n-1,\vec{e}}_{\vec{\tau}_{n-1}<t}$ and $Q^{\vec{e}_j}_{j_n,j_1}(t \mid \vec{\tau}_{n-1})$, which is a probability density, is given by

$$Q^{\vec{e}_j}_{j_n,j_1}(t \mid \vec{\tau}_{n-1}) \equiv q_{j_n j_{n-1}}(t, \tau_{n-1}) ... q_{j_2 j_1}(\tau_2, \tau_1) \tag{4.5}$$

While vector $\vec{e}_j$ represents only a sequence of events, the couple of vectors $(\vec{e}_j, \vec{\tau}_{n-1})$ represents a particular *path* through that sequence. When *j* labels a dynamic state and e_j is a change in the dynamic evolution, the path is associated to a *transient* with events of the sequence occurring at specified times. It should be noted that the integral in Eq. (4.4) extends to all paths in a given sequence. The integrand, Eq. (4.5), is then called the path Q-*kernel* that is determined once we know the set of q[7] and this type of solution is called the ***path and sequence*** approach.

Now, the probability $\pi_{j_n}(t)$ becomes

$$\begin{aligned} \pi_{j_n}(t) &= \int_0^t d\tau_n \varphi_{j_n}(\tau_n) e^{-\int_{\tau_n}^t \sum_{k \neq j_n} p^{\vec{e}_j}_{j_n \to k}(s) ds} = \\ &= \sum_{j_1, \vec{e}_j \neq e_1} \varphi^{in}_{j_1}(\tau_1) \int d\vec{\tau}_n Q^{\vec{e}_j}_{j_n,j_1}(\tau_n \mid \vec{\tau}_{n-1}) e^{-\int_{\tau_n}^t \sum_{k \neq j} p^{\vec{e}_j}_{j \to k}(s) ds} \end{aligned} \tag{4.6}$$

The contribution of a single path to $\pi_{j_n}(t)$ is given by

$$d\pi^{\vec{e}_j}_{\vec{j}}(t : \vec{\tau}_{n-1}) \equiv \varphi^{in}_{j_1}(\tau_1) Q^{\vec{e}_j}_{j_n,j_1}(\tau_n \mid \vec{\tau}_{n-1}) e^{-\int_{\tau_n}^t \sum_{k \neq j} p^{\vec{e}_j}_{j \to k}(s) ds} d\vec{\tau}_n \tag{4.7}$$

This differential magnitude can be properly called *path probability*, that accumulated over the ***damage domain*** (i.e., set of all paths violating DBSL) give us the sequence *exceedance probability*.

[7] See comments on Eq. (4.3) about properties of *q*.

It is obvious that the path and sequence solution is very inefficient unless the number of paths is reduced. However, system protections are usually well designed which means that damage paths are a relatively small number. Stimulus design is essential in reducing the possible paths, as only those activating the stimuli associated to each event in the sequence are possible. The implications of this will be further explored in sections 4.5 and 4.6 below.

Note that $\sum_{\forall \vec{e}_j \neq e_1} \int_{V_{\vec{\tau}_{n-1}<t}^{n-1,\vec{e}}} d\vec{\tau}_{n-1} Q_{j_n,j_1}^{\vec{e}_j}(t \mid \vec{\tau}_{n-1})$ in the solution Eq. (4.4) may be interpreted as the fraction of the injected paths in state j_1 at τ_1 that reach state j_n at t after the sequence of events occurred between τ_1 and t. If the paths are grouped according to some attributes, like for instance paths exceeding DBSL limits (failed paths) we obtain the corresponding attribute frequency, like for instance the exceedance frequency.

These relations also show how sequences may be "chained", i.e., they may be fractioned by accident progression stages, provided certain assumptions makes this fractioned approach valid. This issue will be discussed again in section 4.5.2.2 point ii and in section 6.1.

4.5.2 Application of the path and sequence approach to safety assessments

4.5.2.1 Problem statement. The PSC semi-Markov balance equations

In the general case of previous section, all events are assumed to occur at unspecified times, and there may be many outcomes of an event. When applied to safety assessment in the ISA context, the PSC plant states include a set of *n* safety systems and *k* is any of their corresponding outcomes. Thus, the states *j* and *k* are actually vectors, denoted $\vec{k} \equiv (k_1, k_2, .., k_n)$ indicating that system J_1 is in state k_1, system J_2 is in state k_2 and so on. *N* denotes the number of outcomes, then states, of each system and may be different from one system to another.

$p_{\vec{j}\to\vec{k}}^{e}(t)$ is then strictly meaningless, because transition rates are instantaneous and only "one event at a time" so the transition from $\vec{j}$ to $\vec{k}$ will require at least a sequence of events. They should instead be understood as $p_{\vec{j}_n\to\vec{j}_{n-1}}^{e}(t) = p_{j_n\to k_n}^{e}(t, j_1, .., j_n)$, that is, the transition rate within states of system n, that may depend on the prior to n subsequence. The problem is then governed by several sets of semi-Markov equations, not a single set like in the previous section. Most

important, the rates are strongly influenced by not only time but the process variables.

Thus, the semi-Markov balances Eq. (4.1) are now

$$\frac{d}{dt}\pi_{j_n}(t,\vec{j}_n,\vec{x}) = -\pi_{j_n}(t,\vec{j}_n,\vec{x})\sum_{k_n\neq j_n=1}^{N} p^e_{j_n\to k_n}(t,\vec{j}_n,\vec{x}) + \sum_{k_n\neq j_n=1}^{N} p^e_{k_n\to j_n}(t,\vec{j}_n,\vec{x})\pi_{k_n}(t,\vec{j}_n,\vec{x})$$

$$\sum_{j_n=1}^{N}\pi_{j_n}(t,\vec{x},\vec{j}_n)=1 \quad each\ n \qquad \frac{d\vec{x}}{dt}=\vec{f}_{\vec{j}_n}(\vec{x},t) \quad \tau_{n-1}<t<\tau_n \tag{4.8}$$

with given initial conditions (see below), equations that recognize explicitly the influence of the process variable as well as of the states $\vec{j}_n$ of the plant system configuration (PSC) $\vec{J}_n$(t).

Note that *n* is linked to the time interval, so time zero corresponds to the interval prior to the first dynamic event. The path and sequence solution Eq. (4.4) is also valid, and may be applied for the sequences of events involving any of the PSC states.

Equation (4.8) implies quite restricted conditions. Among other things, the only Markov steady states (i.e., constant in time probabilities) imply recovery rates during long duration intervals, which is an unrealistic situation because, contrary to degradation, recovery is an active, timely action. This means that we need to know a time where $\varphi_{k_1,k_2,..,k_n}$ is known and take it as the zero time initial condition.

This time-zero situation is the start of the plant operation, where all operating/standby systems are assumed in a known plant system configuration, so the system success probabilities are all 1 and the plant process variables are at steady state. For this reason, steady states will be used here to only refer to steady or quasi-steady process variables.

Note that for two-outcome states with $k=1,2$ denoting safe and failed states, $A_1(\tau,t)$, $U_1(\tau,t)$ in Eqs. (4.3) become the system reliability and unreliability and

$$q_{2,1}(\tau,t)\equiv p^e_{1\to 2}(t)R(\tau,t)=\frac{\partial}{\partial t}R(\tau,t) \quad R(\tau,t)\equiv e^{-\int_\tau^t ds\, p^e_{1\to 2}(s)} \tag{4.9}$$

so that each single *q* is determined by the system reliability function, $R(\tau,t)$, while $Q^{\vec{e}_j}_{\vec{j}_n,\vec{j}_1}$ may account for system availability in case that repair events are possible (i.e., some $q_{1,2}(\tau,t)$ are non-zero at some time within the sequence interval). However, they may now depend on the states resulting from prior events.

4.5.2.2 Main difficulties

The main difficulty in solving Eq. (4.8) when applied to real plants lies in:

i. $\vec{J}_n$(t), the plant system configuration (PSC), depends much on absolute time, so it is necessary a clear specification of the systems and the time evolution of the system configuration constituting the plant situation under study, particularly identifying systems that will be connected or disconnected for protection or as a result of failures, i.e., plant reconfigurations. For instance, prior to a reactor trip, the at power configuration is totally different than after the trip, when many systems become disconnected and new ones connected to replace them with the purpose of keeping a steady hot zero power situation. The same occurs if the plant is in a shutdown condition or under reload, the last completely different.

ii. Furthermore, as the accident progress, consistent with the barrier protection main functions, new barrier safety limits and damage domains involving new and more complex stochastic phenomena challenging outer barriers require to consider different associated stages. The damage (failure) domain of one such stage only include paths of the damage (failure) domain associated to barrier safety limits prior in the progression, the nature of the analysis and best estimate codes associated to the different phenomena and sub-problem being different. This fact is exploited via Eq. (4.4) to filter-out many paths, making safety limits damage paths analysis feasible and damage domains small enough. This filtering process is called "*binning*".

    As in the division in problems by plant areas, time scales (see next point) and system configurations do order the progression from fast to slow and from inner to outer barriers. "Plan damage condition" is used to refer to the system configurations under the considered situations, situations that assume some prior barrier safety limits already violated, hence the name. Usually, barrier failures imply strong configuration and dynamic changes, but the plant is not in a steady or quasi-steady process variable state, so it is not the same situation than the period between accidents.

iii. The rates depend on the state $\vec{j}_n$ and process-variables $\vec{x}$. Indeed, the solution in case of a two outcomes (safe and failed, $j_k = (1,2)$), steady process state, with event rates independent on other system states, with known time dependency and no system recovery, is very simple. For $\vec{j}_n \equiv \left(1,1,...,^{n}1\right)$ representing an initial safe state, the probability that the

system continues in its safe state is

$$\pi_{1,1,..,1}(t) = \prod_{k=1}^{n} e^{-\int_0^t p_{1\to 2}^k(\tau)d\tau} \tag{4.10}$$

which simply states that the plant will be totally degraded if no recovery action is taken. As expected, the most important and un-escapable process variable dependency is the one generated by stimuli, see section 4.6.3.

iv. The large amount of components/operational tasks involved in each system configuration, several systems sharing tasks of different interconnected systems, including standby components as well as operating components. Each system is characterized by system functions that may be satisfied by several component configurations, as determined by the system success criteria, which makes the fault tree techniques challenging. In particular, large support systems common to many safety systems.

v. The difficulty of modeling, then computing, the system reliability functions required to compute $q_{j_{n-2}\,j_{n-1}}(\tau_{n-2},\tau_{n-1})$, which is linked to point iv. That is, how to relate the system reliability with the configuration of their components and their failure data.

Some general features of the overall process to solve the risk problem formulated in terms of Eq. (4.8) will be described next and in more detail in section 4.6 and ref. [2].

4.5.3 The importance of time scales. Maintenance time scale and accident time scale

The picture that is at the basis of the reliability models in any PSA and in particular in ISA, is to consider the plant history as a set of sequences of dynamic events, each sequence consisting of an initiating event and its immediate consequences and initiated from the process steady state resulting after the last maintenance and recovery period prior to the occurrence of the initiating event (i.e., in other words, the steady state consistent with the PSC at that time, see section 4.6.1). The immediate consequences include several stages depending on the plant configurations and phenomena, i.e., the stage of the accident progression.

In between two accident (initiator plus immediate consequences) periods, the maintenance and recovery operations occur at a different time scale than during the accident and may be considered as a set of quasi-static events, result of prior accidents that ended-up in a steady state. The maintenance program allows considering the plant history as periodic between reloads, so the

analysis is carried out only during a generic reload period. Changes may be made, though, in the PSA input data to recognize the aging process, in order to make the assumptions more realistic. In the same way, major plant modifications are added in next reload cycles. Considered within the maintenance time scale, the relevant situations are the different modes of plant operation/configurations expected to occur during sufficient amount of time, typically shutdown, reloads, and at power modes.

4.5.4 TSD event modeling features during accident progression

The dynamic events are physical phenomena that occur during the accident progression. Other than the initiating events, that are usually the result of system failures, we have system connections/disconnections and consequential physical phenomena occurring during the mission time. Connection/disconnection events are essential, as they are responsible for the configuration changes of point i in section 4.5.2.2. To better understand the implications, we remind that active safety systems are links between the plant and the environment.

4.5.4.1 Operating systems disconnections and active safety system connections

Consider a plant configuration $\vec{J}_n$ with a standby active system connected to the $\vec{j}_n$ plant configuration state, j_n being the standby system state component. Prior to the disconnection/connection

$$\frac{d\vec{x}}{dt} = \vec{f}_{\vec{j}_{n-2}}(\vec{x}_p, \vec{x}_{disc}, \vec{b}_{n-2}(t)) \quad x_j \in \vec{x}_p \text{ or } x_j \in \vec{x}_{disc} \tag{4.11}$$

where $\vec{j}_{n-2}$, indicates the configuration state prior to the disconnection/connection events, with $\vec{x}_p$, $\vec{x}_{disc}$ the set of process variables included in the remaining, respectively disconnected sections; $\vec{b}_{j_{n-2}}(t)$ denote boundary conditions of the prior configuration, part of the "division in sub-problems" process discussed in section 3.2.3.

The environmental link means that the dynamic model after disconnection of operating systems/connection of active safety systems, has the structure (subscripts *p,s* represent now, respectively the plant variables in the section not disconnected, and the active safety system process variables after connection)

$$\frac{d\vec{x}_p}{dt} = \vec{f}_{j_n}(\vec{x}_p, \vec{u}_n(t), \vec{b}_n(t)) \quad \vec{u}_n(t) = \psi\ (\vec{x}_s, t) \quad \frac{d\vec{x}_s}{dt} = \vec{g}_{j_n}(\vec{x}_s, \vec{v}_n(t)) \tag{4.12}$$

with $\vec{v}$ the system environmental variables, as well as those required to start and operate the active components of the safety system.

The key point is that $\vec{u}_n(t)$ is subject to limits that are precisely the DSSL limits (system success criteria) associated to the barrier safety limit under study and the problem may be decoupled in two independent sub-problems, respectively ensuring DBSL and DSSL (see section 3.1.3). The path and sequence approach may then be limited to the solutions of Eq. (4.8) with either of the dynamics of Eq. (4.12). Note that the configurations are now respectively PSC and SCC so the two problems are different, but of the same kind. In the system alone case, the problem is now easier to solve, and it is possible to increase its level of detail considering subsystems in it so a cascade solution is possible up to a preselected level of detail (see section 4.6.4).

4.5.5 Features of PSA1 sequences

As a result, the PSA level 1 headers involved in the path and sequences approach are physical phenomena headers either induced by plant system reconfigurations including connection of stand-by systems or due to intrinsic phenomena. The intrinsic phenomena are also conditioned by stimuli activations. The active system headers reflect potential system failures upon demand (i.e., stimuli activations and/or subsequent system connection actions). For automatic actions, an automatic change of configurations involving automatic realignments, start-up and warm-up of active system components are expected to be immediate consequence to the events. For operator actions, some of these operations may start at the time of operator stimuli activation, taking place during the delay time prior to actual connection. The operation procedures specify these operator actions, which helps identifying the appropriate ones for each transient path.

For instance, in the case of PSA1 initiating events that start with the plant at power, the protection strategy is first to trip the plant (see section 6.1), which implies to disconnect all the main systems and to connect the necessary ones to keep the plant safe at zero power. The operations involved are mostly automatic, although backup manual actions are also specified in emergency procedures (like procedure E0-ES01 in standard Westinghouse PWR´s). From this zero power configuration, any further consequence of the initiating event that activates stimuli of new safety systems induces an additional change of configuration as a result of its connection.

If the plant does not activate the stimulus for reactor trip, (and the consequential trip of the other main systems like turbine and so on), completely different sequences will be generated than in case of successful trips, and the equivalent system configurations and realignments are anticipated in the abnormal operating and special ATWS procedures. In sections 4.6 and 6.1 below we further clarify this process.

4.6 TSD equations in ISA

4.6.1 Time periods between accidents

Up to now, we have considered plant system configurations and their failures as dynamic events involving plant transients in safety variables, and system success/failure makes reference to the maintenance of barrier safety limits expressed in terms of process variables, that is, success is to keep barrier safety limits conditional on the constraints on $\vec{u}_n(t)$ and $\vec{b}_n(t)$ in Eq. (4.12). In the periods between accidents, however, the process variables are assumed in the steady state consistent with the plant configuration (quasi steady approximation). As a result

$$\frac{d\vec{x}}{dt} = \vec{f}_{\vec{j}_n}(\vec{x},t) = 0 \Rightarrow \vec{x} = \vec{x}_{\vec{j}_n(t)} \tag{4.13}$$

and Eq. (4.8) becomes independent on the process variables, although they evolve in time with the configurations. The path and sequence approach is then unnecessary.

Instead, in order to compute the initial frequencies required by Eq. (4.4), recourse is made to the meaning of a system function and the tasks associated to the components constituting the SCC including human tasks required for its operations (see section 3.1.2)

The plant testing, maintenance and repair operations may guarantee a periodic solution for $\pi_{j_1,j_2,\ldots,j_n}(t)$ with the period extending for a cycle between reloads and the initial configurations corresponding to whether we analyze at power, reload or hot zero power conditions. This makes possible the use of alternative techniques like Fault Trees for stand-by safety systems during non-accident plant operation.

As a conclusion, the system dynamic events as considered in the TSD *dynamic event tree sequences* are of a nature different than events (basic or top) associated to FT/ET (see section 4.6.3).

The great advantage of fault tree-like methods is that although component failure configurations may change with time, the computations depend on the configuration, not on the time it occurs. An additional feature is that components not shared may be factorized. Because safety regulations require operating systems to be separated from safety systems, the operational plant system configurations are also separated. Attention is to be paid when the same systems are used for both purposes, fulfilling the principles thanks to a high reliability of their automatic reconfigurations, as for example, the high pressure pumps of the safety injection system required to keep the system pressure during normal operations, reconfigured as active safety systems in case of activation of accident stimuli.

The details will also be discussed at length in ref. [2].

4.6.2 TSD equations during accidents. Mission times

In order to model the progression, a set of dynamic events, consequence of initiating failures challenging the first safety limit, drive the plant out of the process variable quasi-steady state model of section 4.6.1 and generate sequences of events that are analyzed with the path and sequence formalism.

The simulation is run only for a *mission time* to show that the barrier and system success criteria, conditioned by stimuli activations, are all satisfied within each of the success paths. Barrier failure is assumed if this is not the case during the mission time, so it is equivalent to consider mission time as a common ingredient of the system success criteria for all those safety systems participating in the sequence. From this point on, other progression stages are “chained”, in the sense of the last paragraph of section 4.5.1. In the following, we detail more the path and sequence computation ingredients, mainly event rates.

4.6.2.1 Connection and disconnection event rates

As indicated in section 4.5.4 changes in configurations are essentially due to connection and disconnection events. Connections require a separate, smaller but similar risk assessment analysis, this time for the system only (see section 3.1.3). This analysis compute the system exceedance frequency indicated in Eq. (4.4), $\varphi_k(t)$, that, as mentioned there, is also the frequency of failure during time *t,* when entering a given state at a time zero, in this case the system demand time. However, the demand is conditioned by stimuli activation, of paramount importance (see section

4.6.3 below) and by the delay between the stimulus activation and the time of the action.

As a result, an active safety measure may fail either because the stimulus is not activated, the operator did not succeed in generating a demand for the safety system or the safety system, once demanded, fails in its intervention.

Thus, an appropriate expression to compute *q* in Eq. (4.4) for any safety limit is

$$\begin{aligned} & q^{path}_{j_n,k_n}(\tau,t,\vec{j}_n) \equiv (1-\theta^{path}_{st}(\tau))(1-H^{path}_{j_n,k_n}(t-\tau,\vec{j}_n))\varphi^{path}_{k_n}(\tau,t,\vec{j}_n) \\ & \varphi^{path}_{k_n}(\tau,t,\vec{j}_n) \simeq \varphi^{exceedance}_{k}(T_{mission},\vec{j}_n) \qquad \textit{failure upon demand} \end{aligned} \tag{4.14}$$

Here $\theta^{path}_{st}(\tau)$ is the function that indicates whether or not the stimulus is active at this time in order to account for activations and deactivations. That is, only for times where the stimuli are activated the event may take place. $H^{path}_{j_n,k_n}(t-\tau,\vec{j}_n)$ is the cdf (cumulative distribution function) of the times for operator actions involving the corresponding transitions. Particularly the stimuli activations, but also the success of the operator, are expected to depend on the paths, less so the failure of the system.

Common component/operational safety system tasks involved in the different connecting actions make the failed configurations (quantified by fault trees), embedded in $\varphi^{exceedance}_{k}(T_{mission},\vec{j}_n)$ strongly dependent on $\vec{j}_n$.

Because the safety system reliability is high, success may be approximately considered as certain, and the exceedance frequency of the system separate problem is incorporated only in case of failed safety actions. However, success modifies the sequence configurations, so success headers condition the failed header frequencies, and it is actually the entire FT/ET the one involved (see section 4.6.3).

Note that failure to disconnect or to connect implies that the dynamics follows the same path as before the events. For this reason, the sequence of dynamic events only involve FT/ET success events and the number of dynamic events is only n in a system of n headers. That means that FT/ET sequences are different than, yet related to, dynamic sequences (see section 4.6.3).

4.6.2.2 Reduction of the x dependencies via paths and sequences

4.6.2.2.1 Path dependent component event rates.

In addition to stimuli, very often, component event rates are influenced by process variables. For instance temperatures may alter the rate of a valve to open upon demand. This is taken into account in TSD, because the evolution of variables x on which the rates $p^{e}_{j\to k}(x)$ depend are known for each path,

$$p^{e,path}_{j\to k}(t) \equiv p^{e}_{j\to k}(x_{path}(t)) \tag{4.15}$$

and the problem becomes a particular case of the semi-Markov equations given above.

4.6.2.2.2 Solution of the dynamic dimension of the model. Coupling deterministic and probabilistic aspects.

Equation (4.15) is an example of how to solve the complex dynamic dependencies involved in Eq. (4.8). Once the dynamic paths are identified, which involves solving the dynamic portion of Eq. (4.8), rates become path-dependent as per Eq. (4.15), and the problem becomes but another example of semi-Markov equations, so the contribution of each path is summarized in section 4.5. This is how the ISA-TSD approach handles the x dependency via paths and sequences.

Room is also available in the approach to incorporate operator failure rates via the *H* functions in Eq. (4.14) that are very often path-dependent and should be consistent with the set of plant abnormal and emergency procedures.

The fault trees associated with the events are also factored here, but they are computed at the end of each sequence, to account for common elements and support systems. This important issue is further discussed in section 4.6.3 and ref. [2]. It constitutes a consistent link with classical ET/FT techniques, but keeping the dynamic aspects in mind.

4.6.3 Impact and importance of stimuli. Relationships between FT/ET and DET

A DET may be associated to some ET/FT but they are different concepts, and their respective failure probability computation techniques are also different.

Failed dynamic events imply no change in dynamics, so the number of dynamic sequences in a

DET is the same as the number of dynamic events that are associated to the success headers of a FT/ET sequence. Some static events (do not change the dynamics) in the transient probabilistic space are also crucial, particularly those referring to changes in the state of the activation of the stimuli (activation events), given the fact that activation is required to allow the possibility of the dynamic events.

That means that a FT/ET sequence of $n+m_1$ headers, n being success headers and m_1 failed headers include the same dynamic paths as another FT/ET sequence $n+m_2$. If $m_1>m_2$, the FT/ET sequence frequency is expected lower in the first case, as failed headers imply lower probability, even by order of magnitude. However, the damage they generate is the same.

The state of the stimulus activations of a path allows to discriminate paths with failed headers (that genuinely belong to the FT/ET_{n+m} because they activate the stimulus), from paths with false headers that should not be present because they do not activate; actually the path belongs to the sequence without this header, FT/ET_{n+m-1}, thus increasing the path frequency for the same damage. In other words, activations may discriminate the value of m that should be assigned to the path.

In summary, an essential impact of the activation of stimuli is due to the fact that the more the number of protective events in a sequence, the lower is the sequence contribution to the exceedance frequency. In particular, one failed sequence where a stimulus doesn't activate corresponds to another failed sequence with one protective header less, which increases much the damage path probability. *Thus, to take credit for a header, it is essential to guarantee its stimulus activation. Otherwise the results are non-acceptable from a safety or regulatory stand-point*.

Another important effect of stimuli refers to disconnection activations, as those play an essential role in the time evolution of the PSC.

We finish the section realizing that stochastic physical phenomena, although not induced by active safety system interventions, may also be modeled via Eq. (4.14), with the stimuli being replaced by necessary conditions for their occurrence and the operator action probabilities being interpreted as probabilities of the occurrence of the phenomenon conditioned to the stimulus activation.

4.6.4 ISA application level. Other limitations

When considering the division in sub-problems indicated in section 3.3.3 together with Eqs.

(4.4) and (4.14) they become a hierarchical network of computations throughout the accident progression, ordered according to the principles stated in section 4.5.2.2 point ii. This means that the solution for a PSC is found in terms of the ones solving single safety systems within a sequence.

A safety system in ISA is a dynamic system, that is, its function is modeled in terms of limits in process variables, and ISA is based on the application of the path and sequence approach (see section 4.5) in order to deal with dynamic events, approach only efficient for dynamic sequences including not too many paths. Those are plausible only when accounting for multiple stimuli conditions and header protective measures of high reliability, reducing the size of the failure domains.

Failures due to stimuli not activated, operator actions not taken or failures upon demand are discriminated in an ISA mechanistic description where physical phenomena are detailed, at the price of an increased number of paths, each requiring a FT/ET description. The lowest level of the dynamic subsystems is established when such a detail is considered no longer necessary or adequate, and a manageable set of the failure domain path frequencies may be computed by considering the sub-system function description as a set of SCC whose failure frequencies are handled via the ET/FT associated to the path (see section 4.6.3). Fortunately, most paths may be grouped with a few dynamic attributes sharing the same ET/FTs, accounting for dynamic effects as for instance common dynamic house events.

The selection of the APET sub-problems, their dynamic sequences and the lowest level of the dynamic subsystems is then key when setting up the particular problem. These considerations also limit the scope of applications, ISA being particularly useful for independent V&V.

5. SCAIS: Simulation Code System for ISA

5. SCAIS: Simulation Code System for ISA

Leaving aside the theoretical aspects that inspire the detailed computational methods, ISA analysis involves a lot of transients and its application then requires a set of simulation/computational tools. The computerized platform called SCAIS has been developed for this main purpose. It is composed of 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 day SCAIS (see [32], [33], [34], [35], [36], [37], [38], [39], [40], [41], [42], [43], [44], [45], [46] for its evolution) is the result of a consolidation and modernization program of the prior system. It is being developed in close collaboration with NFQ Solutions S.L., a software development company specialized in risk assessment. Also, the Technical University of Madrid (UPM) actively participates at the testing and application level. Among the objectives of this program are to not only include improvements in technical capabilities but also means to facilitate an easier maintenance and future update.

Section 5.1 presents SCAIS main components, able to manage DET unfolding and communication among the different modules (section 5.2). The main driver, BABIECA, makes an intensive use of code coupling techniques (section 5.4). Section 5.3 describes the particular coupling with SIMPROC, to simulate operator crew actions.

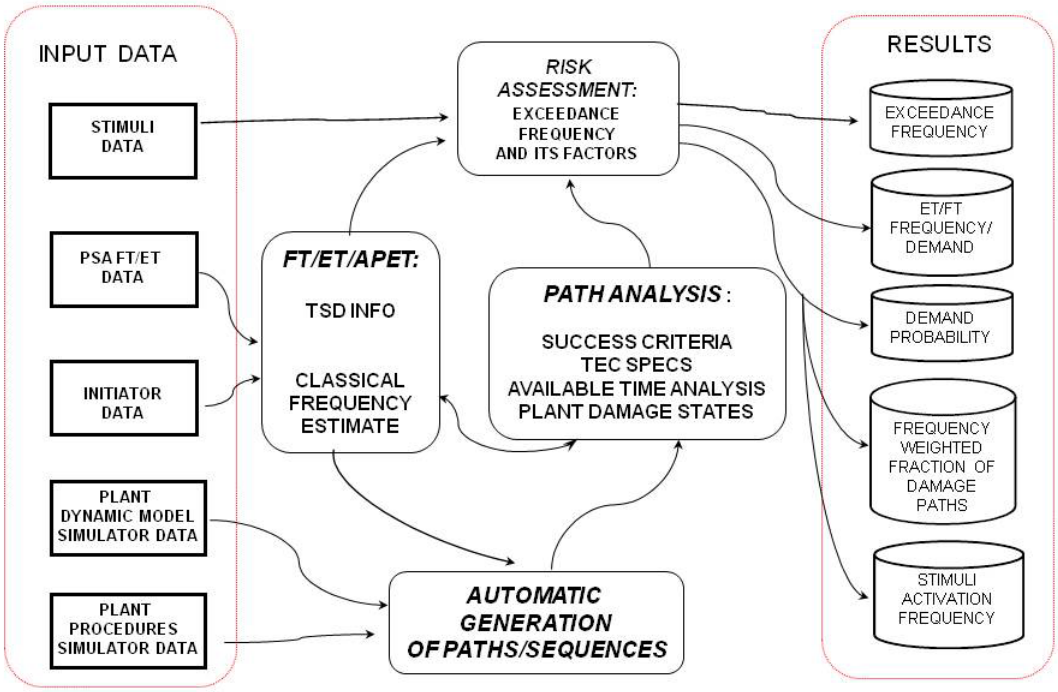

Figure 5. Simplified scheme of the ISA-TSD methodology.

5.1 Main Components of SCAIS

Because the focus of the ISA setup is in DDET transient simulation, most of the components of SCAIS are transient related, while a few others are probabilistic in nature. Figure 5 presents a simplified scheme of the ISA-TSD methodology whose blocks parallel the main components of SCAIS.

The "Automatic Generation of Paths/Sequences" block in Fig. 5 includes the following SCAIS elements:

(1) BABIECA is the general simulation driver ([42], [43], [44], [45]). 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 (see Fig. 6) is the event scheduler that drives the dynamic generation and management of the different event sequences resulting from a given initiating event ([39], [40]). It directs the simulation to perform the systematic traversal of all the possible branches, leading to different sequences. Whenever a branching point (indicated by a set-point crossing) is detected, a request is sent to a decision module in order to know (see section 7) if the simulation of the failed sequence is needed. DENDROS then identifies and manages the branching points and, if the case, asks BABIECA to open new simulation processes, one for each possible outcome of the event (Fig. 6). The result is a DET. DENDROS has been designed to guarantee modularity of the overall system and parallelization of the dynamic event tree generation.

(3) PLANT MODELS. As indicated above, a plant model is a particular user-defined combination of BABIECA modules able to simulate 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 those composed only by internal BABIECA modules ([4], [43], [44], [45]). The possibilities that BABIECA offers to build plant models from its internal or external modules are further discussed 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 ([41]). A more detailed description of the coupling between BABIECA and SIMPROC is described later and illustrated in Fig. 7.

These four SCAIS components implement the main dynamic modules as required by DDET, including also those allowing for the verification of procedures via automatic pilot simulations.

Other SCAIS components are the following:

(5) The PROBABILITY CALCULATOR (ET/FT/APET block in Fig. 5) 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 ([46]).

(6) PATH ANALYSIS MODULE (explicitly shown in Fig. 5), which performs the detailed analysis of individual event tree sequences through the simulation of specific transients (paths) of the analyzed sequence ([29], [46], [47]). In coordination with DENDROS, the PATH ANALYSIS MODULE defines multiple simulation cases, i.e., sequence paths, by varying values of uncertain parameters and/or time delays (human actions or stochastic phenomena). The aim is to identify the sequence failure domain, given the applicable configuration sequence success criteria. 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. Represented by the left-hand and right-hand side columns in Fig. 5, it stores all the input data and results allowing their easy post-process.

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 simulations unless necessary.

(8) The RISK ASSESSMENT module, also shown in Fig. 5, calculates the design barrier Safety Limit Exceedance Frequency, i.e., the frequency of the failed state, by integrating the TSD equations over the failure domain obtained from the PATH ANALYSIS MODULE, and considering the frequency density function obtained from the probability distributions evaluated in the PROBABILITY CALCULATOR ([46]).

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 DETs 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. For the sake of simplicity, only binary branching points are represented where the two output branches correspond to occurrence or not of an event.

Branching criteria are represented by P_i (P_1, P_2, etc) in this figure. They correspond to stimulus activations 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 Fig. 6 represents the opening of new simulation processes while the lower part represents the corresponding dynamic event tree resulting from this procedure.

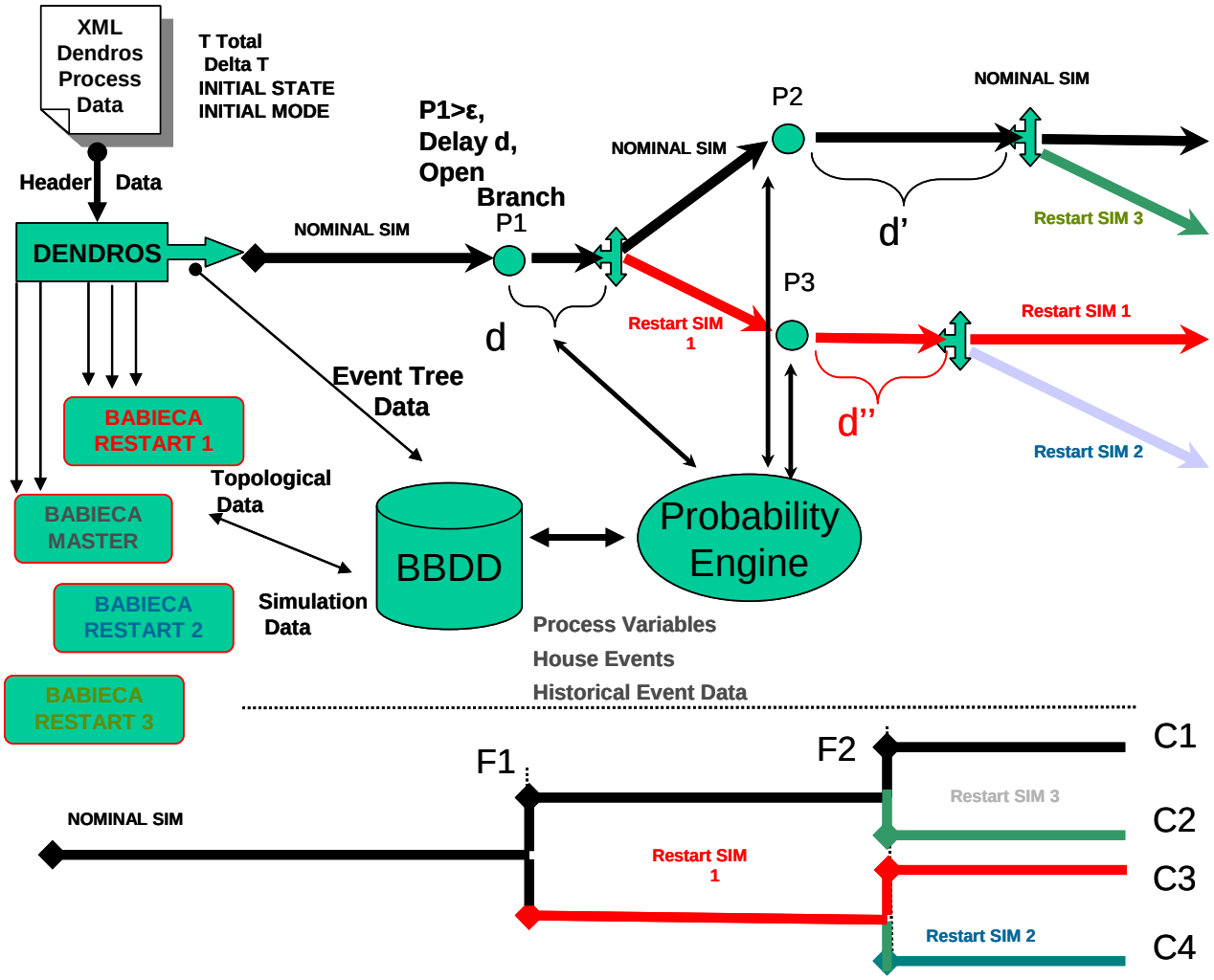

Figure 6. Overall BABIECA-DENDROS-Probability calculator coordination.

5.2 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, as frequently used algorithms, while others can implement some balance equations or a complete model of some plant component such as a heat exchanger or a pressurizer. In particular, the internal module catalogue includes all the modules that resulted from the development of the in-house design-replica codes TRETA (for PWR) and TIZONA (for BWR) ([44], [45]) 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 (Parallel Virtual Machine). 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 thermal-hydraulic or severe accident codes such as RELAP5, TRACE, MELCOR or MAAP can be adapted to work as external modules for BABIECA. Specific wrappers have been already developed for MAAP ([48]), RELAP5 ([43]) and TRACE ([49]).

A particular case of external code connected to BABIECA is the procedure simulator SIMPROC ([41]). 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.

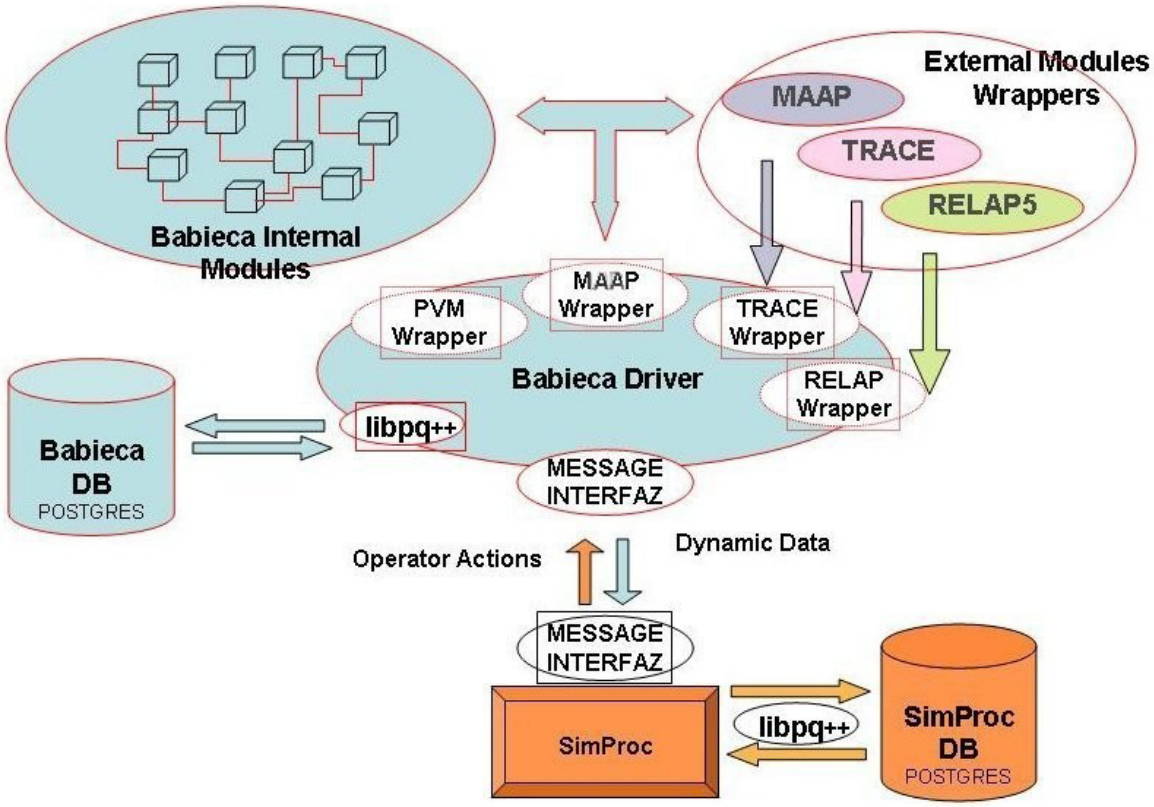

Figure 7. SIMPROC-BABIECA Architecture.

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. It is a part of the general SCAIS data base. SIMPROC has its own data base, independent from the SCAIS data base. More details about SIMPROC are given below.

5.3 SIMPROC

The development of SIMPROC ([41]) has been an initiative of the Spanish Nuclear Safety Council (CSN) in collaboration with Indizen Technologies (today NFQ Solutions) and the Technical University of Madrid (UPM).

The development has been inspired by the operator support system Copma-II ([50]) and its successor Copma-III ([51]) developed at the OECD-Halden Reactor Project (HRP). Some of the functionalities of SIMPROC were already implemented in the adaptations of Copma-II ([52]) and Copma-III ([53]) for simulation developed by CSN and UPM in collaboration with HRP.

SIMPROC provides capability to simulate the interaction between operators (guided by procedures) and the plant (represented by dynamic simulation models). This way, more comprehensive analysis tools can be developed in order to:

1. Evaluate the adequacy of emergency procedures for preventing the degradation of accidental situations.
2. Improve the probabilistic evaluation of human actions in PSA through a better treatment of their associated uncertainties which, in many cases, dominate over other sources of uncertainty and cannot be ignored.

SIMPROC has been specifically developed for analysis of EOP. Modeling SAMG strategies is a more complex task which could require some extensions of the current SIMPROC capabilities.

5.3.1 SIMPROC Approach

Plant simulations have been frequently used for analysis of operator actions and procedures. The usual approach is to use the built-in capabilities of the plant simulation code to model operator actions. In some cases (e.g., MAAP), there are provisions to specifically model

operator actions, possibly conditioned to the occurrence of specified plant conditions. In other cases (e.g., RELAP5, TRACE), user configurable control systems are used to emulate operator actions. In both cases the resulting simulation capabilities are equivalent and quite limited.

A different approach has been used for SIMPROC which has been developed as an independent tool. Interactions between humans and plant are treated at computer process level. SIMPROC and the plant simulator run in parallel and exchange information during the simulation. This way, the simulation capabilities are greatly improved without increasing the complexity of the simulation codes and their input decks. Only a communication module needs to be added to the simulation code in order to allow coupling to SIMPROC. A message passing protocol, namely PVM, is used for bi-directional communication between SIMPROC and the plant simulator. A significant advantage of this approach is that the very same procedure can be used with any plant simulation code, provided that it is coupled to SIMPROC.

Since the aim is to evaluate procedures, not operators, SIMPROC is not an operator model but a procedure model. Very few assumptions are made about the operator behavior, basically consisting on assuming that procedures are followed by ideal operators. Nevertheless, SIMPROC has been developed taking into account the possibility of future improvements including coupling with HRA cognitive models which could act as a filter/modifier on the SIMPROC output.

5.3.2 SIMPROC Methodology

Procedures in SIMPROC are modeled as a set of steps and steps consist of a set of instructions. Instructions are the basic modeling elements of a procedure. The concept of step as a set of related instructions is introduced to better emulate real procedures. Several procedures can be modeled in a simulation session. As a general rule, steps and instructions in a given procedure are executed in sequential order except when a sequence changing instruction is found.

Although a procedure is a consistent set of instructions oriented to a particular objective, the sequence of actions performed by operators does not necessarily start at the beginning of a procedure and does not necessarily include actions from a single procedure. The concept of activity is included in SIMPROC to represent a particular sequence of actions with well-defined starting and ending points, belonging to the same or different procedures.

Procedures are modeled in SIMPROC on the basis of a catalogue of available instruction types. In its current state, available instructions are:

- ACTION: Specifies an action or a manipulation to be performed on a component.
- AUTOCHECK: It is a flow control instruction with a typical IF-THEN-ELSE structure. A logic condition is evaluated and, depending on the result, the THEN (true result) or the ELSE (false result) part of the instruction is executed. Inputs to the logic condition can be other logic variables or comparison functions involving process variables and/or constant setpoints. Both the THEN and the ELSE part of the instruction may contain, at most, a single GOSUB GOTO or INITIATE instruction (see below). If an empty THEN or ELSE part is reached the procedure execution continues with the next sequential instruction in the procedure.
- INITIATE: Creates a new activity starting at the indicated procedure instruction.
- FINISH: Terminates an activity.
- GOSUB: Causes the control flow to jump to a specific instruction in the procedure, allowing for a later return to the calling point upon execution of a RETURN instruction.
- GOTO: Causes the control flow to jump to a specified instruction without keeping memory of the calling point.
- MONITOR: Similar to an AUTOCHECK but the condition is monitored in the background during a specified time interval. If the logic condition becomes true at any time in the monitoring interval, the THEN part of the instruction is immediately executed. If the logic condition remains false the ELSE part is executed upon termination of the monitoring interval.
- RETURN: Causes the control flow to return to the first instruction following the last executed GOSUB.
- WAIT: Prevents the execution of the next instruction until the indicated time interval expires or the specified process condition is met.

Codified procedures that can be understood by SIMPROC are written in XML. Procedures can be codified to the desired level of detail and the codification rules and tags allow maintaining the main structure of the original procedure in the codified version. This allows for an easy verification of the correspondence between original and codified procedures. In addition, the codified procedure is a well structured separate file instead of a section or even a set of disjoint lines in the input deck of a plant simulation code. This also allows for a more efficient management and

maintenance of codified procedures.

Times in SIMPROC are measured in terms of simulation time which is one of the variables that SIMPROC receives from the plant simulator. Each procedure instruction has three associated attributes which determine the procedure execution speed. These attributes are:

- SKILL: Role of the operator who should execute the action. Currently there are two skills defined in SIMPROC: REACTOR and TURBINE. It would be possible to define additional roles such as AUX, TURBINE2, etc.
- TEXEC: Time that the operator needs to execute the instruction. It is implemented as a delay before the action becomes effective. This delay does not include hardware delays (such as opening time of a valve) that should be modeled in the plant simulator if necessary.
- TASKLOAD: Degree of business of the operator during the execution of the instruction (i.e., during TEXEC). It is measured in percent units. A single operator is able to execute several instructions simultaneously, provided that the accumulated TASKLOAD remains lower than 100. If the operator is asked to execute a new instruction that would make his accumulated TASKLOAD greater than 100, execution is delayed until some ongoing instruction is finished and the TASKLOAD of the new instruction can be allocated.

A special pseudo-procedure is always used consisting of a set of monitor instructions checking for entry conditions in actual procedures with a “forever” monitoring interval. This pseudo procedure is loaded and executed at the beginning of the simulation and when an entry condition is detected, the THEN part of the corresponding monitor initiates the required procedure.

5.3.3 SIMPROC Structure and External Interface

The main components of SIMPROC are:

- SimProcDriver is the main process, also responsible for communication with other system components and external processes. EOPs are loaded at start-up along with the monitor pseudo-procedure for entry conditions which is immediately executed. During the simulation process SimProcDriver communicates regularly with the plant simulator to obtain process information and to send actuation orders when so required by the procedures.
- SimProcDB is the database to store all data related with operating procedures as well as the procedure simulation results.

- The XML interface parses the input files and the codified procedures and stores the information in SimProcDB.
- Items are the modules which perform specific operator tasks required by instructions in procedures.

Connecting SIMPROC to a simulation code requires developing some interface functions in both codes, such that they can exchange meaningful information. In the development of SIMPROC connection to MAAP has been used as a prototype. However, in order to improve flexibility, they have not been directly connected but through BABIECA, the intermediate simulation engine.

5.4 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. These concepts are further developed in [43].

6. Nuclear applications. TSD deterministic verifications

6. Nuclear applications. TSD deterministic verifications

6.1 The nuclear binning process. Modeling and grouping initiators

As a general rule, the protective strategy of industrial plants is to disconnect the plant from the network that it is serving, then to take internal safety measures to counteract safety problems. The two major safety problems to face in Nuclear Barrier Safety assessment is first to stop neutron power generation and second to remove decay heat. The main difference between both is the widely different magnitude and time scales of both thermal power sources. While the neutron power contribution is close to 97% in average and the chain reaction phenomena are in the scale of seconds to minutes, decay power accounts for less that 7 per cent and associated thermal-hydraulic phenomena are in the scales of hours. This emphasizes that, in order to preserve barrier integrity under accident conditions, the first safety function to be achieved is sub-criticality, (that constitute the first binning stage), and, additionally, that in the treatment of the rest, the preceding stage may be considered quasi-instantaneous. We further elaborate this below.

6.1.1 Sub criticality safety function and main system trips

Equations (4.4) are valid for the first progression stage. The fuel safety limits are those challenging the fuel integrity. They result from applying tight bands to the “specified acceptable fuel design limits” (SAFDL). The first and most important required safety function is to ensure sub-criticality. Because the time scale of reactor power transient is small (scale of minutes) mission time is also small.

Initiators include internal and external events. We only deal here with internal ones. Typical internal initiators are failures of the control systems or unbalances in reactivity-inducing process variables. Prior to the initiator, the plant is operating at a process steady state compatible with the power level and control system modes.

Reactor and main plant system trips are the main protective headers guaranteeing sufficient sub-criticality by ensuring final steady states at zero power without manual actions. The initiators are of high frequency and the trips are then designed with high reliability. Stimulus design for tripping main systems, like reactor and turbine, are most delicate and include a set of redundant and diverse signals usually called trip functions. Aside from the reactor trip measure, most

important protective measures are key main system disconnections and safety system connections. Although in the long time scale it may be considered short, the number of events involving system reconfigurations makes this safety issue to be considered in its own short time scale.

The exceedance frequency limits are most stringent, as exceedance situations become precursors of potential degradations. Failure to generate the reactor trip signals either because of hardware failure of the protection system signal generation or because the process variables do not activate the trip functions imply the need to simulate situations with potential abnormal final states at power[8] or showing sufficient intrinsic reactivity removal as to make the situation subcritical without further manual actions. The abnormal at-power final state case becomes then a specific PSA sub-problem (severe accidents criticality studies), while the second is considered together with the case where reactor trip signals work but the reactor trip safety system fails to insert the rods. (Anticipated Transients Without Scram, ATWS).

6.1.2 Other PSA level 1 internal initiating events

Two major consequences of the main plant system trips are major changes in plant systems and component configurations as well as a narrow band of after trip process variable values, $\vec{x}_{ST}$, that are constrained, in addition to zero power, by the subcritical equations

$$\vec{x}(T) = \textit{plant steady state} \qquad \vec{x}(T+\Delta t_{trip}) = \vec{x}_{ST} \quad \rho(\vec{x}(T)) = 0$$

$$\sum_{l=0} \int_{T}^{T+\Delta t_{trip}} \frac{\partial \rho}{\partial x_l}(\vec{x}(t)) \frac{dx_l}{dt} dt = \sum_{l=0} \int_{T}^{T+\Delta t_{trip}} \frac{\partial \rho}{\partial x_l} f_{l,\vec{j}_N}(\vec{x}(t),t) dt < 0 \tag{6.1}$$

Here $\rho(\vec{x}(t))$ is the reactivity, and the index l includes all variables controlling external reactivity (control rod position, boron concentration, etc) as well as intrinsic (fuel and coolant temperatures and density including voids). Thus, in the decay heat time scale, variations of $\vec{x}_{ST}$, initial situations of the second binning stage, from one initiator to another, may be considered as uncertain around typical values and all the initiating paths that trip the reactor may be grouped together in a single group with frequency

[8] A typical example would be the case where the turbine does not trip in a PWR that may induce via the control systems a fast increase of the reactor neutron flux/power in case of negative reactivity coefficients. In the same way, a typical example of an ATWS with milder consequences (but challenging the SAFDL design limits) is a rod drop accident in a PWR when the fallen rod or rod bank is located such that it goes undetected or detected but not exceeding trip set-points. As another example, a secondary system pipe break may in certain situations induce an uncontrolled cooling, generating intrinsic reactivity able to overcome the shutdown margin (return to criticality).

$$\varphi_0^{PSA1}(T) = \sum_{in} p_{1\to 2}^{in}(T)\pi_1(T, \vec{x}_{in}(T)) \qquad \text{(internal initiators)} \qquad (6.2)$$

neglecting the trip time as small in the new time scale. This is the basis of the modeling/computation of the initiating events of the next binning period, the PSA level 1 sequences challenging the rest of the safety limits and critical safety functions other than sub-criticality. A similar process may be applied to group ATWS initiators that shutdown the power via intrinsic feedback, if disconnection of the main plant systems does not fail. Otherwise, specific groups should handle the specific configurations created by some scenarios.

6.1.3 Other binning stages

The quasi-static (maintenance) and the quasi instantaneous (reactor trip) periods exemplify two of the grouping techniques of initiators and simplifications of the TSD equations (see sections 4.5 and 4.6). They are typical of the similar process followed with other binning stages, part of the division in sub-problems illustrated before in the PSA level 2 case. For instance, shock phenomena are instantaneous, but severe core degradation includes large time scales.

The initiator frequency is taken to be the exceedance frequency of the prior binning stage, grouping those damage paths with compatible time scale and configuration modes. Equations (4.4) and (4.14) are then used within any progression stage. More details about the exact connection with, and how to incorporate the results of, the classical FT/ET plant models will be given in ref. [2]. Thus, in practice the initiators of other than the first accident progression stage are not component failures, but grouped situations coming from prior stages.

6.1.4 External events

Other types of initiators are induced by external events that are not included here (see section 4.1). The major difference is that a single external event is a “common cause” of several internal plant initiators, with strong implications in the initiator frequency, configuration sequences and the combination of potentially catastrophic scenarios. A unified TSD treatment is not available and it is excluded from this contribution.

6.2 Applications to DSA, PSA1 and PSA2. Consistency verification

By considering both, sequences and transients, and by lowering the sequence analysis to

transient level, the ISA-TSD methodology is able to address most of the important issues involved in DSA and PSA (see section 4.6). It allows performing different types of consistency checks which can refer either to the internal consistency of similar types of analysis or to the cross consistency of different types. Of particular importance is the possibility of checking the consistency between DSA and PSA level 1 to ensure that success criteria used in both types of analysis are compatible (see section 4.6.2).

6.2.1 Checking issues in DSA

One of the main issues with DSA is whether the set of analyzed Design Basis Transients (Accidents), DBT(A)s, actually configures an envelope of all the possible plant transients (accidents) complying with the design basis assumptions. Note that DSA groups transients and accidents in a reduced number of classes. Each class is characterized by a level of severity, expressed in terms of a particular set of DBSL limits that should not be exceeded and by an expected frequency, usually stated in terms of qualitative likelihood (for instance, one or more transients of a given class can be expected during a calendar year). Consequently, a specific set of DBT(A)s is defined for each class which must envelop all the transients (accidents) of that class.

Verifying envelopes without depending on the designer methods is possible by identifying the transient space that should be enveloped by the DBT(A)s, which results from considering a particular set of the uncertainties considered in section 4.4.1. Such verification would consist of checking that all the failure domains of the DSA sequences are empty.

For cases where a Best Estimate Plus Uncertainty (BEPU) approach has been used in DSA, uncertainties in the DSA transient space should be characterized with probability distributions. In this case, the DSA transient space is also a probability space and the exceedance frequency of the class DBSL can be evaluated. The envelope verification in this case would consist of checking that the exceedance frequency is consistent with the tolerance levels allowed in the BEPU analysis ([54]).

Together with checks of the DBSL barrier safety limits, similar checks may be made to verify the system functions, this time using the DSSL instead of the DBSL applied to the separate systems, to verify the safety system design features reported in the safety analysis reports.

6.2.2 Checking success criteria, available times and minimal system configurations in PSA Level 1

As discussed in sections 3.2.1 and 3.2.3, PSA1 success criteria include available times and minimal safety system configurations.

Concerning available times, the ISA damage domains (see section 7) are conditional on system success, i.e., any success event in a failed path assumes that the associated safety system function is satisfied and its stimulus is activated. That means that the path frequency is conditional on this assumption. Therefore, available times being the difference between the path times of stimuli activation and the execution event times defining the path, checks may be done by computing the stimuli activation domains, so an available time domain is obtained for each action. The proposed PSA1 available times should then be higher than any of the ISA values.

Concerning confirmation of minimal configurations, the design safety system limits (DSSL) should be satisfied for the success headers of the PSA1. If the plant models used in the Dynamic Event Tree (DET) unfolding (see section 5.1) include the safety system represented by a particular header, this condition may be verified as another output of the simulation.

Although this approach leads to a lot of different system configurations, each with an associated dynamic model of the safety systems (including several possible modes of operation), for purposes of verifying the deterministic aspect, i.e. whether or not maintenance of DSSL limits guarantees DBSL limit, it is an adequate check. However, unless all configurations are considered, the exceedance frequency calculations cannot be compared with PSA1 results.

This said, since stand-by safety systems considered in PSA1 are all interface systems with environment, it is possible to divide the problem into two (see sections 4.2 and 3.3.3) and the separate problems may also be analyzed,

(1) using the system function DSSL of plant-system common process variables as boundary conditions of the plant separate model, then checking the DBSL.

(2) Checking the DSSL with a separate system model, but including all possible configurations.

with the additional advantage of checking also design assumptions about non safety graded active safety systems considered in the emergency procedures.

Examples have been already given in references [1] and [3].

6.2.3 Checking other deterministic issues in PSA (Levels 1 and 2)

Deterministic issues to be checked in any PSA, aside envelope issues, available times, minimal configurations, sequence and success criteria, discussed before, are the verification of stimuli activations (see section 4.5.3) and the delineation of sequences, i.e., the structure of event trees.

Checking sequence delineation consists of verifying that no dynamic event is included in a sequence without previous (or simultaneous) activation of its stimulus. At the same time, it must be verified that whenever the stimulus of a dynamic event is activated, a branching point appears in the sequence for considering the possibility that the dynamic event actually occurs.

These ISA envelope and delineation verification techniques may be applied to any sub-problem of the PSA2, (including PSA1 as the first progression stage; see section 4.6.2) by considering the boundary condition variables as safety variables. Once their damage domains conditional to APET attributes (see section 3.3) are identified (see section 7) we may check the deterministic aspects of the APET unfolding.

Examples of those are given in references [1], [2] and [3], and sections 7 and 8. Specialized techniques in case of event timing and boundary conditions may be useful, if not inevitable, for PSA2 (afforded in sections 7 and 8).

6.3 Verifying emergency operating procedures and severe accident guidelines

When verification of an EOP for scenarios without core melt is the issue, simulations are run with an automatic pilot version of that EOP, as realistic as possible, by using the procedure simulator SIMPROC (see [41] and section 5.3) coupled to the automatic event tree SCAIS simulator. Timing of 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 verified. If this is not the case, the procedure is questioned at specific points. Examples are given in references [1], [9], [35], [36] and [38]. They may be part of the automatic sequence delineation verification of PSA1 stage 1 (see sections 3.2.2 and 4.3).

As explained before, accident progression stages imply different safety limits challenging different, subsequent barriers as a result of different degrading phenomena. To verify how these may develop when following severe accident guidelines, we have chosen a similar to Fukushima

scenario of total blackout, simulating the expected strategies.

6.3.1 Case Example. Impact of Severe Accident Management Actions (SMAGs). Station Blackout (SBO) sequences

A SBO sequence in a PWR-Westinghouse plant starts with the loss of both off-site and on-site (Emergency Diesel Generators, EDG) AC power ([55]). The SBO signal triggers the reactor SCRAM, turbine and RCP trip, as well as Main Feedwater (MFW) pump (turbine driven) trip due to low steam pressure. Additionally, under these conditions only accumulators (ACC) are available for emergency core cooling, since the high-pressure and low-pressure safety injection (HPSI and LPSI) systems need AC power. These systems, as well as the containment spray and fan coolers, are not available until the eventual AC recovery. Another eventuality that aggravates the scenario is the possible leak through the RCP seals. As long as AC is not recovered on time and the seal LOCA occurs, the RCS inventory will decrease uncontrolled, and therefore core uncovery will result.

Availability of DC power is initially assumed upon the AC power loss but battery depletion leads to loss of DC power at an uncertain time if AC power is not recovered. It is assumed that availability of DC power is guaranteed as soon as AC is recovered since battery chargers fed by AC power start working immediately.

In this analysis, the SCAIS-MAAP platform is used to simulate SBO sequences including the main human actions required by EOP E-0, ECA-0.0, E-1, ES-1.2 and FR-C.1. Further in the sequence, SAMG actions, corresponding to SAG-1, SAG-2 and SAG-3, are considered as well. Figure 8 is a schematic representation of the AM strategies involved in SBO sequences. Depending on AC recovery, and DC availability, it indicates the applicable EOP/SAG, the method for steam generator level control (“Level” box), the state of safety injection systems (“HPSI/LPSI” box) and the resulting cooling method (“Cooling” box).

For example, once the seal LOCA occurs along the scenario, if the AC power has been recovered (left column of Fig. 8) the operating crew follows EOPs corresponding to LOCA sequences, namely, E-1 or ES-1.2. Level control of steam generators is performed by using the AFW motor driven pumps and both high pressure and low pressure injection systems are available. Unless otherwise required, cooling is performed at a maximum rate of 55ºK/hour. However, if the core exit temperature (CET) exceeds a critical value (922ºK), changing to fast cooling is required. This implies a full opening of SG power operated relief valves (PORVs), and would indicate the

transition to SAMG.

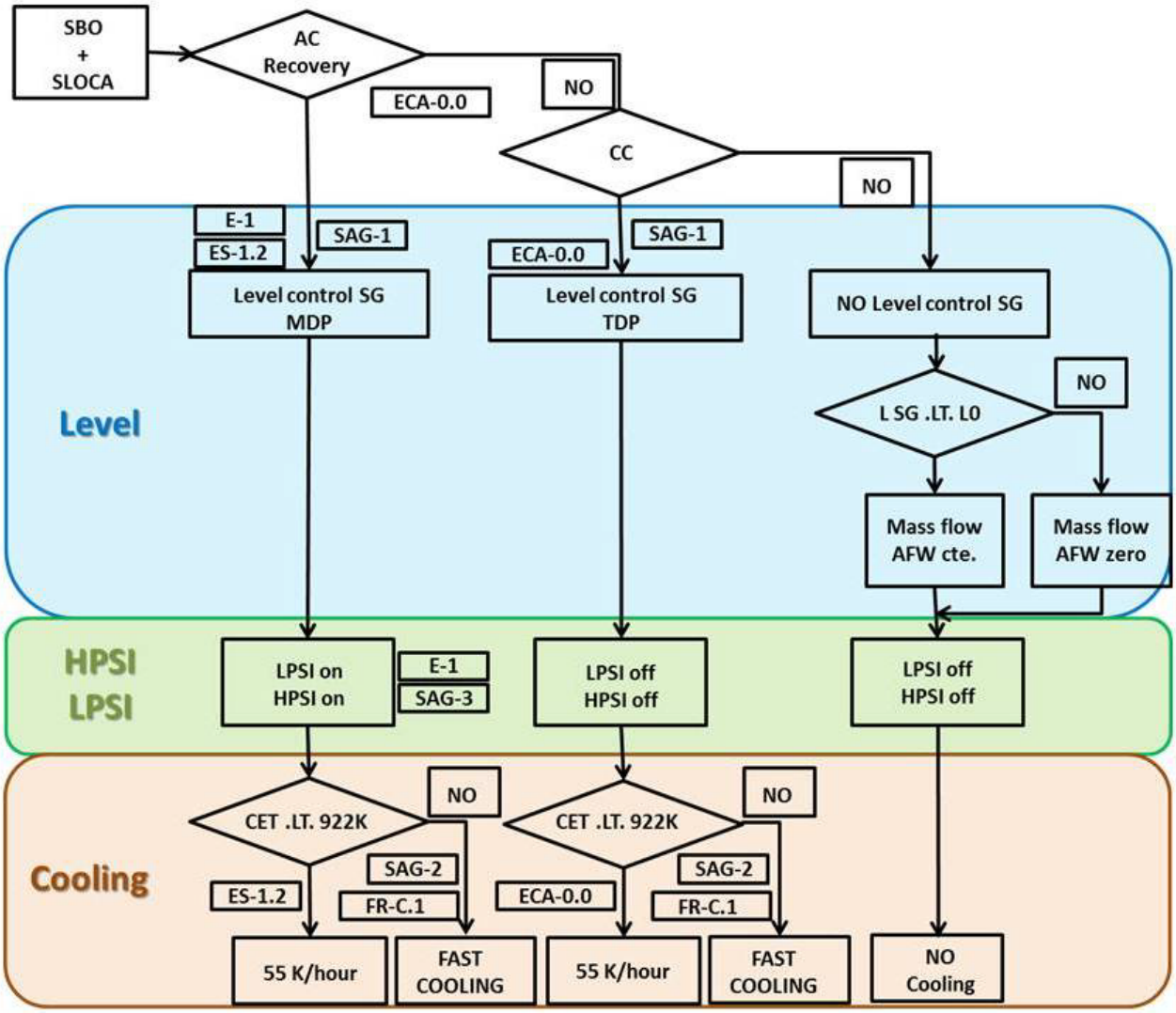

Figure 8. Main operator actions taken into account in SBO sequences with seal LOCA.

Since the objective of the analysis is to verify the adequacy of procedures and guides, no human error has been considered. It is assumed that all the actions are performed by an efficient and qualified operation team.

The purpose of the analysis was to ascertain the beneficial effect of the fast cooling operation when the limit of 922ºK CET is exceeded. The analyzed sequence was the loss of AC power followed by seal LOCA and loss of DC power before the AC recovery. Time uncertainty in DC loss and AC recovery has been considered since these times may strongly condition the efficiency of

the AM measures.

Five damage indicators have been considered in the analysis:

1. Core uncovery,
2. CET above limit (CET> 922ºK),
3. PCT above limit (PCT > 1477ºK),
4. Fuel relocation in lower plenum, and
5. Reactor Pressure Vessel (RPV) failure

These damage indicators are sorted by severity, and each simulated path of the sequence (identified by a combination of DC loss time t_0, and AC recovery time t_1) is characterized by the most severe damage indicator reached along the path. Figure 9 shows the so called Multiple Damage Domains (MDD) which result when only slow cooling is considered (upper graph) and when the fast cooling strategy is allowed (lower graph). Each point (t_1, t_0) in these graphs represents a simulation run and its color indicates the highest severity indicator reached along the path, according to the following code: red for core uncovery, blue for inadequate core cooling, CET>922ºK; orange for cladding embrittlement, PCT>1477ºK; purple for fuel relocation in lower plenum and black for vessel failure).

Note that for all the simulation paths $t_1 \geq t_0$ and, therefore, all the points in the graphs are located below the diagonal line $t_0 = t_1$.

The upper graph MDD of Fig. 9 has been obtained by performing nearly 850 MAAP simulations and taking into account only EOPs (E-0, ECA-0.0, E-1 and ES-1.2) with slow cooling (55ºK/hour) by means of SG and AFW. Results show the final state of the plant for each path. The right hand boundary of the plotted MDD represents points where the vessel fails at the time of AC recovery. Points located further to the right side of this boundary correspond therefore to paths where the vessel is already failed when AC is recovered. No path has been simulated in this area and, therefore, no point is plotted in it but it must be understood that the whole region belongs to the vessel failure domain and, therefore, all the other damage indicators have been also exceeded.

The lower graph MDD of Fig. 9 has been obtained with 750 simulation runs considering fast cooling by means of SG PORVs (from SAG-2 action).

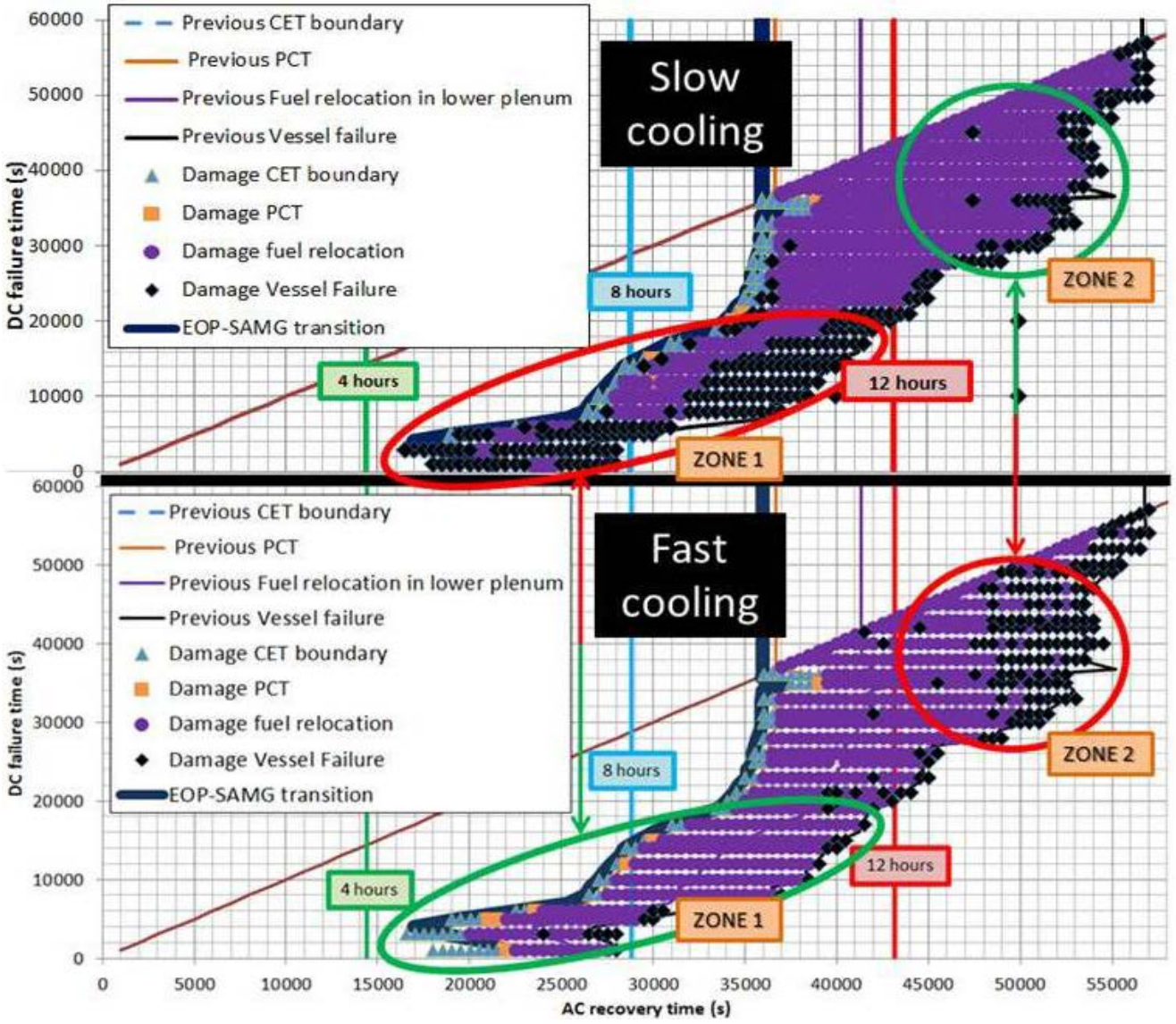

Figure 9. Comparison between MDDs with slow and fast cooling.

Comparison among both MDD (slow and fast cooling) allows measuring the impact of the application of this AM action. In Fig. 9 ([55]) two differentiated zones (Zone 1 and 2) show up in this comparison:

1. Zone 1 allows concluding that if AC is recovered relatively early after core uncovery (t< 3 hours) then fast cooling is an efficient strategy in order to avoid vessel failure.
2. However, if the AC power is recovered later (Zone 2) the application of fast cooling would not be recommendable since it results in a higher number of paths leading to vessel failure.

7. Damage domain assessment

7. Damage domain assessments

As shown in section 4, TSD has a deterministic aspect, i.e., finding the damage (failure) domains and a probabilistic one, i.e., finding its frequency.

The SCAIS transient simulation techniques described in section 5 do not include the strategy to optimize the branching approach of the DET to minimize the number of runs needed to identify damage domains. Remind that damage domains are the locus of failed transients differing only on specified features characteristic of the uncertainty problem (see section 4.4.2). We will illustrate here the case of the uncertainty of the timing of events. New techniques were explored by CSN/MOSI and a proposal was presented in the appendix of ref. [3]. Other well-known techniques may be applied to parameter uncertainty, including envelopes of initial conditions ([56]). Section 8 will deal with the boundary condition uncertainty.

Section 7.1 presents the main structure of the off-line TSD prototype, used as a developmental tool for testing ISA/SCAIS improvements, in particular event timing issues. The prototype performance has been exemplified under some challenging situations, like (section 7.2) the impact on the containment of an inflow of hydrogen and steam as a PSA2 sub-problem, resulting from a severe accident medium size LOCA; and in a totally different case (section 7.3) consisting on a plant transient analysis (SAR type) in an experimental facility, to show the unified character of the tools.

7.1 Developmental tools. Testing ISA/SCAIS improvements with an off-line TSD prototype

Figure 10 shows the structure of a first prototype ([27], [28], [46], [47], [57], [58]) to implement the search of damage/failure domains and the computation of the exceedance frequency. This way, each research item can be tested off-line before its integration in SCAIS.

It is easy to distinguish circles dealing with single transients (paths) from those related to the overall strategy, i.e., selection of paths and identification of failure domains. Several search methods have been proposed and tested (appendix of [3], and [27], [28], [46], [47], [59]).

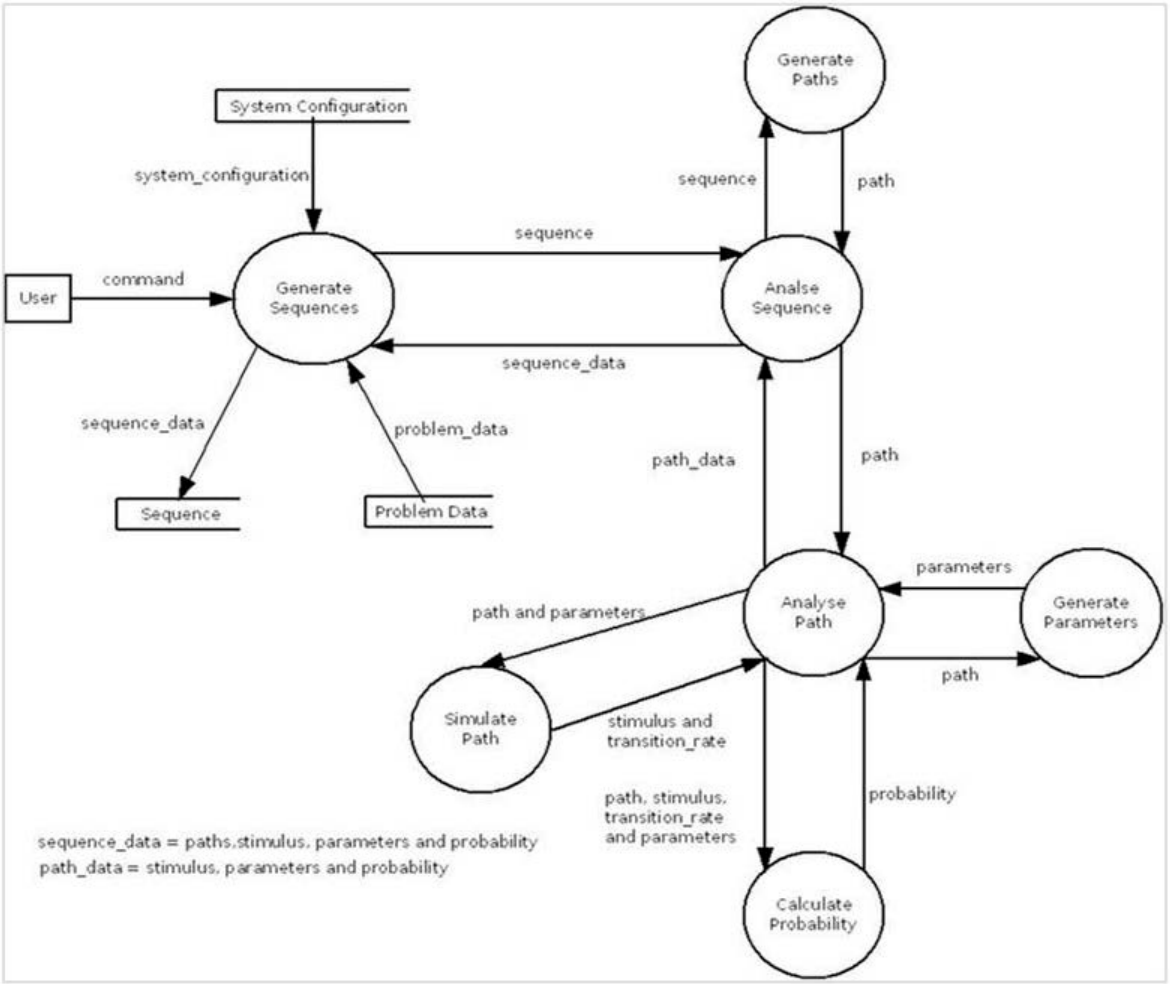

Figure 10. Structural block diagram of TSD prototype.

Concerning transient treatment, the “simulate path” action in Fig. 10 is performed with the help of suitable models for finding reasonable envelopes (adequate models). They may be found in many ways (from BE to simplified, surrogate or parametric models, see section 8).

7.2 Stochastic H2 ignition in containment as a result of a medium size LOCA without safety injection

Figure 11 shows the problem and the scenario setup. Stimulus variables for H2 combustion in containment are those characterizing the onset of flammability conditions for containment gas mixtures. Actual occurrence of the phenomenon, however, requires also an ignition source. This has been modeled random, with ignition pdf’s depending on electric supply conditions. Figure 11 lists the available safety systems, that generate sequences of transitions with recurrent combustions, as may be seen in the results. Sequences are identified in Fig. 11 and Table 1 as bracketed lists of

events identified by number (see the event list in Fig. 11). In this study an adequate model with two versions, a very simplified approach with dubious internal physical consistency as described in [27], and an enlarged model basically equivalent to the MAAP TH-laminar combustion modeling ([57], [58], [60]). Table 1 shows some comparison of the results obtained with both models.

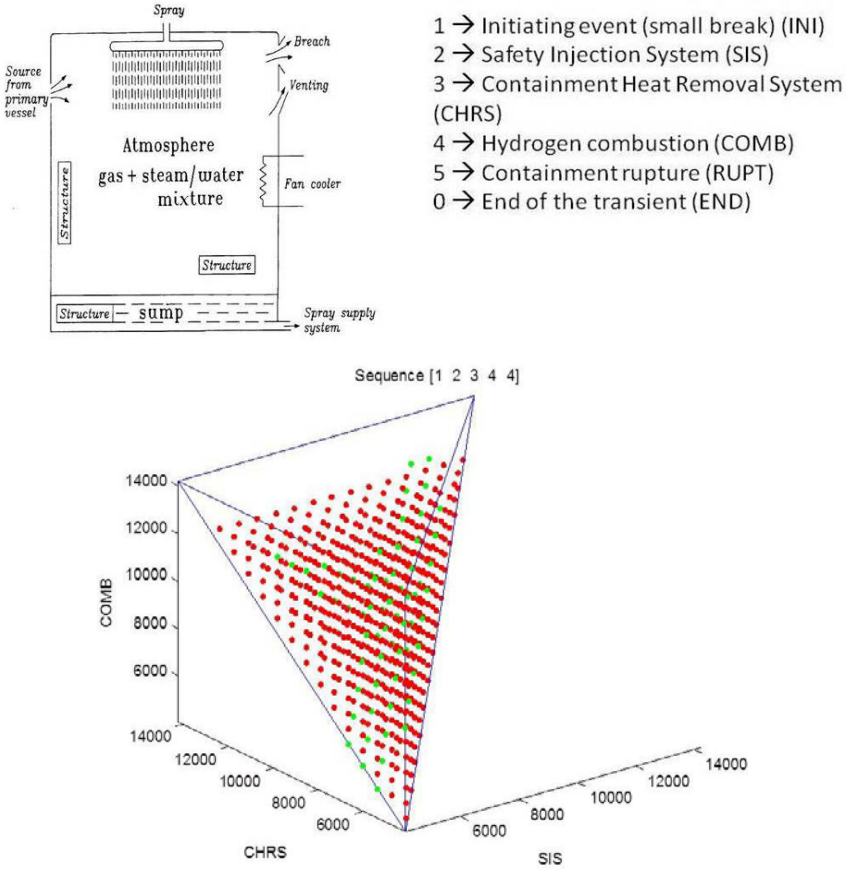

Figure 11. Containment pressure failure domain of sequence [1 2 3 4 4].

Table 1. Conditional probabilities[9] of sequences [1 2], [1 2 3], [1 2 3 4], [1 2 3 4 4].

		simplified model	***enlarged model***
COMB	**[1 2]**	0.0824	0.0495
	[1 2 3]	0.0206	0.0111
RUPT	**[1 2 3 4]**	0.0399	0.0088
	[1 2 3 4 4]	Impossible	0.0073

[9] I.e., failure exceedance frequency divided by the frequency of the initiator.

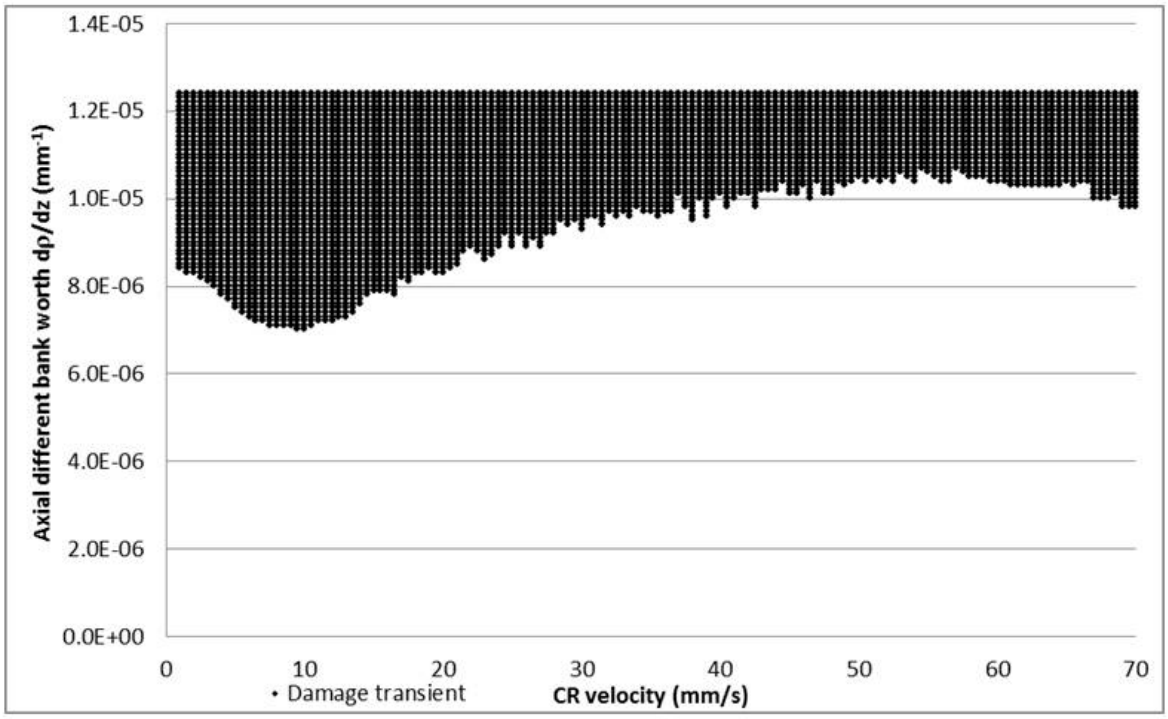

Figure 12. Damage Domain for the control rod withdrawal transient.

7.3 Damage domains of the High-Temperature Test Reactor (HTTR)

A 30MWth prototype High-Temperature Engineering Test Reactor (HTTR) is being operated by the Japan Atomic Energy Agency (JAEA). One of the design basis transients reported in the SAR of this reactor is the uncontrolled control rod (CR) withdrawal from subcritical conditions. The analysis of this accident was assessed with ISA methods ([59], [60]). An adequate model implemented in the code HTTR5+/GASTEMP was developed, and its results compared with those of the JAEA Safety Analysis Report. The code parallels the equivalent JAEA counterpart ([60]), with the HTTR5 module accounting for the chain reaction aspects and the GASTEMP module for the gas coolant thermal-hydraulics. Comparison confirmed adequacy of the model for the reference DBT transients.

A search for damage domains was then tried with two different sampling methods (random sampling and parameter scanning). From the results (some of them presented in Fig. 12), the following conclusions were drawn:

(1) Consistency between the results obtained using the two different sampling methods is confirmed.

(2) In case the reactor scram does not actuate when demanded, (Anticipated Transient without Scram), damage is predicted to occur when axial differential bank reactivity worth equals or exceeds 7.01E-6.

(3) However, no transient path is found in the damage domain that would not lead to the high neutron flux/power reactor scram signal (105.5% of the nominal). The damage domain is therefore expected to have a low frequency, as it requires failure of the reactor scram system.

(4) The most unfavorable combination is an axial bank differential reactivity worth of 7.01E-6 (mm-1) and bank speed of 10 (mm/s), as a result of the combination of separate reactivity effects. This checked the enveloping character of this analysis case.

(5) Calculation time for the random sampling method is longer than for the parameter scanning method, because the former handles more ‘‘safe/no-damage’’ transients, additional to the “damage” transients which are the only contributors to the failure exceedance frequency.

(6) In this study, only around 40% of all transients that belong to the control rod withdrawal from subcritical condition sequence in HTTR are predicted to be damage transients while the remaining 60% are safe transients.

8. Path assessment and boundary condition uncertainty

8. Path assessment and boundary condition uncertainty

ISA TSD method requires adequate dynamic models, able to find reasonable envelopes for any sub-problem describing accident progression phases in different areas of the plant. However, best estimate codes are too large and complex to be used directly and finding adequate models for each sub-problem is hard and difficult to validate, especially when considering the widely different phenomena involved from one sub-problem to another. CSN-MOSI is working on a new approach to tackle this. This section presents the status of the development.

Because the safety variables of interest are not that many, the idea is to use the BE multi-process-variable codes to identify and feed Enveloping Surrogate Dynamic Models (see also section 9.1.2) that are adequate to project and envelope the BE result on any preselected single process-variable. The single process variable surrogate models are dynamic models based on piecewise linear approximations and have the same math structure in all cases. Very fast and efficient algorithms allow running the very many transients required to afford the timing and boundary condition envelopes. The basis for the dynamic surrogate models is the Transmission Functions Theory (TFT) ([30], [31]). Section 8.1 is devoted to the definition of Transmission Functions (Funciones de Transmisión or FT) and its combined use with the TSD approach described in section 4.5. Section 8.2 describes the mathematical framework of the theory. Further properties and discussion are presented as well in section 9.1.

8.1 TFT+TSD approach

The rationale of the TFT is simple. As it is well known, dynamic linear systems in the interval $(T, T+\tau)$ may be described by the matrix of transfer functions $\left[G_2(s)\right]$ with elements $G_2^{j,i}(s)$ such that

$$x_j(\tau+T) = L^{-1}_{y\to\tau}\left\{\sum_{inputs\ u_i} G_2^{j,i}(y)\left[\tilde{u}_i^2(y) + x_i(T)\right]\right\} \tag{8.1}$$

with $L_{\tau\to y}$ $L^{-1}_{y\to\tau}$ the Laplace operator so time is τ and $y = j\omega$ with ω the frequency variable.

When iterated for a two-piece linear system, assuming continuity of vector $x_i(T)$, it leads to

$$x_j(\tau+T)=\left\{L^{-1}_{y\to\tau}\sum_{inputs\ u_i^2}G_2^{j,i}(\tilde{y})\tilde{u}_i^2(\tilde{y})+\right.$$
$$\left.+\ L^{-1}_{\tilde{y}\to\tau,s\to T}\sum_{inputs\ u_i^1}\sum_{k=1}^{N}G_2^{j,k}(\tilde{y})G_1^{k,i}(s)\tilde{u}_i^1(s)\right\} \tag{8.2}$$

Each term provides the contribution of the input in each interval to the second interval of the output. This idea is generalized for a piecewise linear system of *M* pieces in order to describe the dynamics of process variable x_j. As indicated in Fig. 13, Transmission Functions (FT in Fig. 13) provide the contribution $x_{j,i}$ of a given input u_i (i.e., boundary condition variable) to a given process variable x_j (as for instance pressure) via products of transfer function matrices in different Laplace variables ($[G_1(s_1)]$, $[G_2(s_2)]$, …. in the figure), each modeling the dynamics associated to each of the time intervals between dynamic events in a sequence.

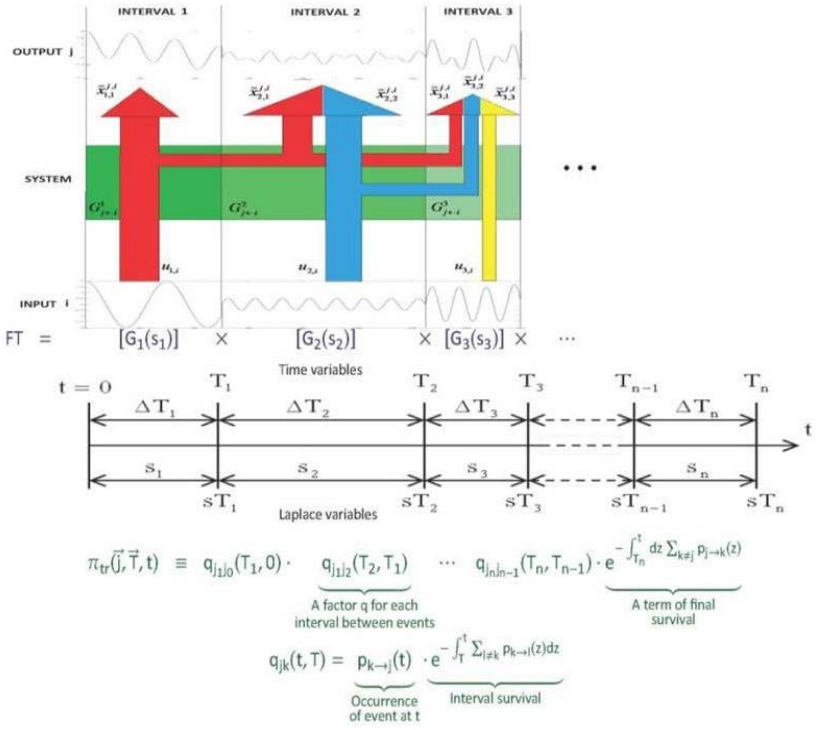

Figure 13. TFT+TSD approach.

Figure 13 also summarizes TFT+TSD and its relation to each other. The figure only tries to visually correlate the relationships within the intervals of the sequences. The actual equations are described in section 4.5 and Eqs. (8.3) to (8.7) below. Taken together, they are adequate to compute the contribution of a given path to the failure exceedance frequency, using TFT for each safety variable, which allows to ascertain the stimuli activations as well as the failed or success state

of safety systems and barrier safety limits.

8.2 TFT equations

Although correct, the matrix products of transfer functions in Eqs. (8.1) and (8.2) are usually intractable. However, the theory is able to find an alternate description based on well-known Frobenius techniques ([30], [31]), that allows very fast algorithms for their computation in the time domain. The surrogate model provides the time evolution along a sequence of events (see Fig. 13) followed by the process variable $x_j(t)$ as

$$\begin{aligned}
&x_j(t) = \sum_{inputs\ i} x_{j,i}(t) \\
&x_{j,i}(t) = L^{-1}_{in\ \text{all y,s}}\left[\sum_{m=1}^{M} FT^{j,i}_{n+1,m}(\tilde{y}_{n+1}, s_{n,m})\tilde{u}^i_m(s_m) \right] \\
&t = T_n + \tau_{n+1} \\
&0 < \tau_{n+1} < \infty \\
&s_{n,m} \equiv (s_n, s_{n-1}, ..s_m) \equiv (s_{n,l}, s_{l,m})
\end{aligned} \tag{8.3}$$

with no matrix products, only the same *j*,*i* pairs involved in all intervals.

By inverting to the time domain for any time partition and boundary condition time shapes given by the input functions, we recover any of the multiple transient paths associated to the uncertainty in time and boundary conditions, keeping everything else the same. Contrary to other surrogate models ([61]) but compatible with them, the alternate description of the FTs have a physical meaning in terms of the SOEs (see also sections 9.1.1 and 9.1.2) that states explicitly the essential aspects of the dynamics:

- First, rather than involving all members of the $\left[G_{n+1}(\tilde{y}_{n+1})\right]$ matrix as in the product approach, the alternate treatment deals only with the ingredients associated to its $G^{j,i}_{n+1}(y_{n+1})$ component, i.e., the polynomials $Q^{j,i}_{n+1}(y_{n+1})$ and the characteristic polynomials $P_{n+1}(y_{n+1})$

$$G_{n+1}(\tilde{y}_{n+1}) \equiv \frac{Q_{n+1}(\tilde{y}_{n+1})}{P_{n+1}(\tilde{y}_{n+1})} = FT_{n+1,n+1}(\tilde{y}_{n+1}) \tag{8.4}$$

For this reason we drop indices *i,j* in Eq. (8.3) in the following.

- Second, each event in the sequence is represented by a coupling *NxN* matrix [*R*], *N* being the order of the system (see section 9.1.2 for its physical meaning). Matrix [*R*] may be computed from the original set of transfer functions, but the purpose here is to identify them with experimental or BE results.
- Third, the chain operation coupling the intervals is relatively simple and has recursion relations in both the n index (that advance in time) as well as the m index (that change to another FT of the same variable).

The alternate description is, for $n \neq m$, with $s_{n,m} \equiv (s_n, s_{n-1}, ..s_m) \equiv (s_{n,l}, s_{l,m})$ the Laplace variables of any partition of time t associated to the sequences

$$FT_{n+1,m}(\tilde{y}_{n+1}, s_{n,m}) = \sum_{q=0}^{N-1} \mathbb{Z}_q^{n+1}(\tilde{y}_{n+1}) W_q^{n,m}(s_{n,m})$$
$$\mathbb{Z}_q^{n+1}(\tilde{y}_{n+1}) \equiv \sum_{m'=0}^{q} \sum_{l=q+1}^{N} \left(p_l^{n+1} Q_{m'}^{n+1} - Q_l^{n+1} p_{m'}^{n+1} \right) \frac{\tilde{y}_{n+1}^{\,l+m'-(q+1)}}{P_{n+1}(\tilde{y}_{n+1})} \tag{8.5}$$

where $\mathbb{Z}_q^{n+1}(\tilde{y}_{n+1})$ is a transfer function defined by Eq. (8.5) and built with Q_l^{n+1} and p_l^{n+1} the coefficients of the polynomials defining $G_{n+1}(\tilde{y}_{n+1})$, and $W_k^{n,m}(s_{n,m})$ is computed via the following recurrence relation in index *n*.

$$W_k^{n,m}(s_{n,m}) = \sum_{q=0}^{N-1} \mathbb{R}_q^{n,k}(s_n) W_q^{n-1,m}(s_{n-1,m}) \quad n = m+1, m+2, ...$$
$$W_k^{m,m}(s_m) = \frac{\sum_{l=0}^{N-1} R_{k,l}^m s_m^l}{P_m(s_m)} \tag{8.6}$$
$$\mathbb{R}_q^{n,k}(s_n) \equiv \sum_{m'=0}^{q} \sum_{l=q+1}^{N} \left(p_l^n R_{k,m'}^n - R_{k,l}^n p_{m'} \right) \frac{s_n^{\,l+m'-(q+1)}}{P_n(s_n)}$$

A similar recurrence relation helps as well to compute the FT for different *m*. These equations are converted to efficient algorithms that prove TFT as a time and boundary condition uncertainty approach complementary to the traditional parameter uncertainty techniques that cover the rest (initial conditions and key parameters). TFT algorithms are being tested in the SCAIS prototype, by replacing the adequate models, i.e., inserting them in the “simulate path” module in Fig. 10.

8.3 Verification through an example: Point Kinetics Nuclear Reactor model

To address a significant testing example, we consider a sequence of nuclear chain reaction transitions due to control rod insertions-extractions in startup tests of nuclear facilities. This example is chosen because there are many studies on the Nuclear Reactor Point Kinetics (PK) model (see reference [62]) that provide comparisons and because the PK without feedback is an example of piecewise linear systems as follows.

The vector of process variables include a set of concentrations of families of radioactive isotopes generated as a result of fissions products, able to produce delayed neutrons, together with the very fast additional neutron production that is direct result of the fissions themselves. Fissions are generated with a multiplicative factor, the reactivity $\rho(t)$, from a neutron flux $\phi(t)$, basically proportional to the total number of fissions. Then, the corresponding state vector is described by components:

$$\begin{cases} x_j(t) = C_j(t) & \text{Precursor isotope concentration of family j (j=1, ..., N)} \\ x_N(t) = \phi(t) & \text{Nuclear reactor neutron flux} \end{cases} \tag{8.7}$$

The features of the multiplicative reactor change *ρ(t)*. In order to measure *ρ*, a set of experiments changing its value $\rho(t) = \rho_n$ during given time intervals $T_{n-1} < t < T_n$, are performed, inferring the reactivity values from the time evolution of the neutron flux. The experiments are made at sufficiently low flux level as to prevent that any feedback mechanism introduces simultaneous, intrinsic reactivity changes. The experiment thus fails if the neutron flux reaches an excessive value.

We can consider a six precursor groups PK model in a three intervals sequence[10]:

1. First interval has null initial conditions, is subcritical, and a constant source input signal is applied.
2. Second interval lasts 400 time units, is supercritical and input signal is maintained.
3. Third interval lasts 600 time units, is subcritical and the input signal is still maintained.

Taking into account the previous hypothesis, the dynamic matrices of the system are:

[10] Values of parameters, times, and input functions are in range but arbitrary, just for demonstration purposes. They are not representative of any actual reactor or transient.

$$[A_n]=\begin{pmatrix} \beta_1/\ell & -\lambda_1 & 0 & 0 & 0 & 0 & 0 \\ \beta_2/\ell & 0 & -\lambda_2 & 0 & 0 & 0 & 0 \\ \beta_3/\ell & 0 & 0 & -\lambda_3 & 0 & 0 & 0 \\ \beta_4/\ell & 0 & 0 & 0 & -\lambda_4 & 0 & 0 \\ \beta_5/\ell & 0 & 0 & 0 & 0 & -\lambda_5 & 0 \\ \beta_6/\ell & 0 & 0 & 0 & 0 & 0 & -\lambda_6 \\ (\rho^n-1)\dfrac{\beta}{\ell} & \lambda_1 & \lambda_2 & \lambda_3 & \lambda_4 & \lambda_5 & \lambda_6 \end{pmatrix} \qquad (8.8)$$

$$[B_n]=[I_7]$$

and where

$$\begin{cases} 1/\lambda_j = \text{average time of the group j to produce a delayed neutron after any fission} \\ \beta_j = \text{fraction of the total number of neutrons per fission born from decay of group j} \\ \beta=\sum_{j=1}^{6}\beta_j = \text{total delayed fraction} \\ \ell = \text{period time for fast neutrons to born after a fission} \\ \rho^n = \text{reactivity of interval n in dollars \$ (1\$=}\beta) \end{cases} \qquad (8.9)$$

The routine developed implements the application of Frobenius method, solves the FT recurrence relations and generates the graphical comparisons with the FT matrix method results. A realistic set of parameters (to a certain extent) has been chosen, and a change of the total fraction of delayed neutrons β from 0.007 to 0.006 in the last interval has been simulated to introduce a deeper discontinuity.

Interval	β_1	β_2	β_3	β_4	β_5	β_6	ℓ	ρ(\$)
1	*0,0003*	*0,0013*	*0,0011*	*0,0024*	*0,0012*	*0,0006*	*4 10 $^{-6}$ s*	**-0.01**
2	*0,0003*	*0,0013*	*0,0011*	*0,0024*	*0,0012*	*0,0006*	*4 10 $^{-6}$ s*	**+0.01**
3	*0,0002*	*0,0012*	*0,0010*	*0,0021*	*0,0010*	*0,0005*	*4 10 $^{-6}$ s*	**-0.02**

and $\lambda_1 = 0{,}0133\ s^{-1}$; $\lambda_2 = 0{,}0325\ s^{-1}$; $\lambda_3 = 0{,}1219\ s^{-1}$; $\lambda_4 = 0{,}3169\ s^{-1}$; $\lambda_5 = 0{,}9886\ s^{-1}$; $\lambda_6 = 2{,}9544\ s^{-1}$.

As expected, the error is very much higher than before, since the amount of operations has increased significantly. In any case its value is around 10^{-8} %.

This no feedback PK model illustrates well the capability of the Transmission Functions method to reproduce discontinuities. Figure 6 shows the results when different sojourn times in the three intervals are taken and the input is the same step in the three intervals. Because the $[R]$ matrix of the two first intervals is unity (the $Q^n_{j\leftarrow i}(s_n)$ polynomials may easily be checked to be the same for *n=1,2*, as well as the input) no discontinuity in derivatives is expected, while discontinuous derivatives should appear in-between the second and third intervals due to different beta fractions,

inducing $[R]$ different than unity.

However, as seen in Fig. 14, apparent steps (discontinuity in the variables) at the two first transitions times are also observed. Those are actually due to the stiffness (large differences in the poles of the transfer functions, i.e., the roots of the polynomials $P^n(s_n)$ in the denominators of the transfer functions) of the PK model that includes large negative poles.

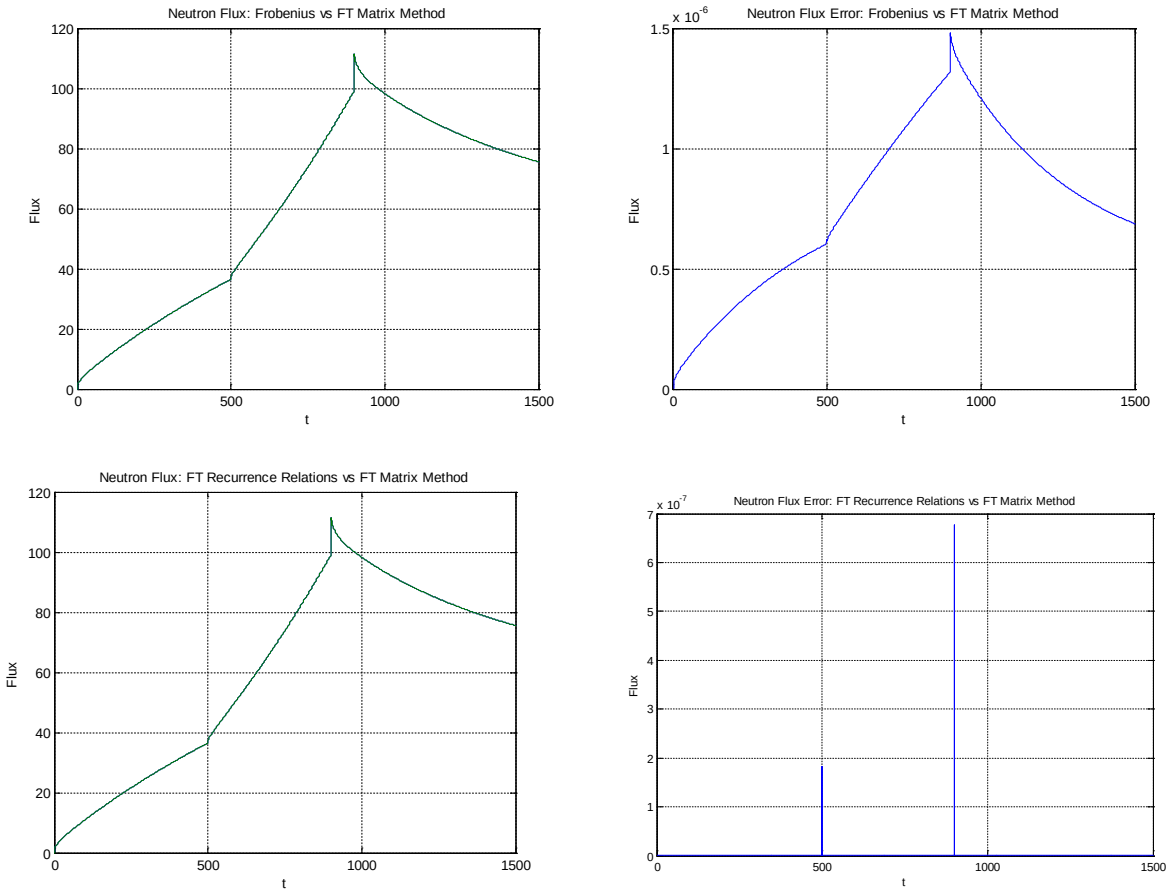

Figure 14: Point Kinetics 6 groups/3 intervals: Methods comparison (flux and absolute error vs time) (up) Frobenius vs FT matrix method; (down) FT recurrence relations vs FT matrix method.

In summary we have three different sources of discontinuities, clearly discriminated by the theory:

i. Discontinuities of the input.

ii. Apparent discontinuities in the variables due to stiffness of $P^n(s_n)$.

iii. Discontinuities of the variable derivatives due to $[R]$ matrix differing from identity.

9. Future developments. Conclusions

9. Future developments. Conclusions

In this section we suggest further research directions (section 9.1) and summarize the main conclusions (section 9.2) of this review paper.

9.1 ISA road map development. TFT and IDPSA

Section 9.1.1 delineates different research aspects of TFT, while section 9.1.2 relates ISA to the more general DSA+PSA techniques being developed worldwide ([63]), indicating some topics to borrow/lend from/to them.

9.1.1 TFT research Path 1: Further PSA-TFT conceptual developments

In the context of TFT, it is possible to define several useful figures of merit to synthesize results of PSA dynamic assessments, paralleling similar ones in ET/FT. For instance, header-importance indices may characterize its dynamic efficiency, i.e., the degree its action, when executed, curves down (protecting) or up (degrading) the trajectories of the safety variables in a given sequence. This verifies and measures the protective or degrading actual function of the header. For instance, a header associated to a safety system designed to cope with a given DBSL safety limit, may behave as degrading for other DBSL, or if in other place of a sequence.

As another example, when time intervals are large enough, (as qualified by the spectrum of roots of the characteristic polynomials), a sequence analysis may be simplified (and coupling gains may be defined by evaluating the $\lim_{s_n \to 0} \mathbb{R}_q^{n,k}(s_n)$), to establish regions where the damage domain becomes insensible to the duration of the interval. In the same way, for large τ_{n+1}, it is simple to evaluate the asymptotic value of all transmission functions, $FT_{n+1,m}(y_{n+1} = 0, s_{n,m})$ to determine a minimum success domain where the safety limit is not violated, a necessary condition for any after sequence steady state.

9.1.2 TFT research Path 2: FT envelope identification techniques

The physical meaning of the [*R*] matrices (see second bullet in section 8.2) may be clarified. When they are the identity matrix, all the derivatives of the process variable (representing the trend of the evolution) remain unchanged from before to after the event, i.e., the event is

dynamically inefficient. The coupling transfer functions $\mathbb{R}_q^{n,k}(s_n)$ are in this case determined only by the characteristic polynomials ($P_n(s_n)$ in Eqs. of section 8).

That means that the experimental/BE evidence of dynamic events, characterized by fast changes in trends, is well captured with the deviation from identity of the [*R*] matrices, while the uniform evolution continuous behavior in-between events may be described by quasi continuous changes only in the characteristic polynomials. Within one such uniform interval, the condition [*R*]=[*I*] defines an analytical prolongation, similar to the well-known in single piece linear systems. With the implication that the Hilbert transform (HT) techniques ([64]) that are familiar to find envelopes in uniform signal flow processing may be applied as well to this extension to multi-variables piecewise linear systems.

This is further encouraged when considering the similarity of TFT with the wavelet simulation technology. It is quite obvious that TFT overcomes the limitations of Fourier transforms and the like, due to high derivatives, because in TFT theory they are explicitly described. The wavelet approach includes an expansion in a multi-resolution wavelet orthogonal basis, as well as a translation operation to describe neighboring intervals, based on a time displacement of the wavelets basis. In the more specific context of describing piece-wise linear systems via TFT though, both the wavelet form and the translation operation are naturally given by the interval transfer functions. Thus the application of wavelets identification techniques looks particularly appropriate ([65]).

HT envelopes of the experimental/BE results, within each interval, whether Laplace based or wavelets based, may be easily computed and this information used to identify, for given R matrices, single characteristic polynomials of that interval, that envelop the experimental/BE results. This is the meaning of FTs as “envelope surrogate models“, specifically adapted to the nature of sequences of dynamic events. The identification will be based on a representative and in-depth[11] post-processed ([66], [67]) set of transient cases run with BE codes in SCAIS for several sequence time partitions with their results stored in its transient data base. The same runs may be used to identify all safety variables.

On the other hand, FTs are an extension of linear systems to piecewise linear ones that keep the nice features for the treatment of model topology division invoked in section 3.3.3 within each

[11] The set of transients to include in the SCAIS data base should be quality-graded runs that may scale to the plant scenarios. The direct use of the BE codes is not recommended.

interval. It means that decomposition and synthesis of sub-problems are rigorously described by detailed block diagrams that provide surrogate models for other variables, starting from those in smaller sub-systems.

9.1.3 TFT research Path 3: Application to estimates of source terms in PSA2

The U.S. Nuclear Regulatory Commission (NRC) representative PSA2 study ([14], [17], [68], [69]) estimates uncertainty bands for the release of the most important families of radio-nuclides. The approach is basically the same as the main idea of the TFT surrogate models, using in their case a data base of results of radiological inventories obtained by BE codes, to fit a surrogate model. However, these surrogates are too crude and do not capture properly the dynamics, questioning the surrogate results.

9.1.4 Integrated DSA and PSA

For each variable *x* involved in the transition rates, $p^{\mathbf{e}}_{k\to j}(x)$ (in Eqs. of section 4.5), the transient results of the adequate or surrogate models convert them into time variable rates as required by the TSD. This establishes a link of ISA/TSD[12] with other approaches based on dynamic reliability, like IDPSA (Integrated Deterministic and Probabilistic Safety Assessment, see [19], [63]), whose major point is the treatment of the dependence of these rates on process variables. A common IDPSA practitioner´s concern is big data results instead of knowledge. Indeed, in the process of exploration of the uncertainty space, ISA can generate hundreds of transient simulations. Interpretation and understanding of the physics and logic behind sequences may be a formidable challenge, prompting for big data visualization techniques (see [70], [71] and Fig. 9 as an example).

Therefore, it is important to equip SCAIS with adequate data mining and classification techniques, which would help to establish lossless extraction and condensation of useful information amenable to expert evaluation. In this context, TFT may be considered as another post-processing technique picturing significant results from a protection perspective, providing further incentive for TFT PSA conceptualizations.

9.2 Conclusions

We have reviewed the history and evolution of quantitative risk assessment methods in the

[12] See section 4.6.2.2.1.

nuclear field as well as the parallel, ISA unified approach followed by CSN MOSI for the independent verification of the industry quantitative assessments. The review included the development of ISA theory and models as well as the SCAIS computer platform and its prototype for testing. New ideas to handle the important event timing and boundary conditions uncertainty that allows dividing and synthesizing results of the overall PSA2 accident progression were presented. Several examples of its applications to real size plants and experimental facilities were given. They promise a realistic approach to afford the hard to handle problem of analyzing consequences of sequences of events under large uncertainties in large systems while ensuring consistency.

The usually obscure treatment of time in conventional PSA sequences is made transparent. One important conclusion is the need to explicitly incorporate the impact of stimuli for protective actions in the reliability computations. Failure to do it increases the likelihood of systematic and unacceptable underestimates of the failure exceedance frequencies. Incorporating them requires affording the challenge of a tightly coupled deterministic and probabilistic mutual influence. The unified ISA method presented here is among the simplest procedures that captures these features in a feasible way.

10. References

10. References

[1] J.M. Izquierdo et al. (CSN), 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 publication, Colección Otros Documentos, 40.2016.

[2] J.M. Izquierdo et al. (CSN), CSN Experience in the Development and Application of a Computer Platform to Verify Consistency of Deterministic and Probabilistic Licensing Safety Cases. Volume II. Probabilistic Developments and Applications, submitted to be published at CSN publication, Colección "Otros Documentos", 2016.

[3] J.M. Izquierdo et al. (CSN), The Problem of Safety Margin Assessment within the Risk Informed Regulation, submitted to be published at CSN publication, Colección "Otros Documentos", 2016.

[4] Izquierdo J.M., Hortal J., Sánchez M., Meléndez E., Why sequence dynamics matters in PSA: Checking consistency of probabilistic and deterministic analyses, chapter published in Advanced Concepts in Nuclear Energy Risk Assessment and Management, T. Aldemir, Ed. World Scientific Publishing Company Pte. Ltd (2016).

[5] USNRC, Annual Update of the Risk-Informed Activities Public Web-Site, SECY-15-0135, October, 2015.

[6] USNRC, Risk-Informed Activities, http://www.nrc.gov/about-nrc/regulatory/risk-informed/rpp.html

[7] USNRC, Probabilistic Risk Assessment Reference Document, NUREG-1050, September, 1984.

[8] J. W. Hickman et al., PRA Procedures Guide. A Guide to the Performance of Probabilistic Risk Assessments for Power Plants, NUREG/CR-2300, Vols. 1 and 2, 1983.

[9] J.M. Izquierdo et al. (CSN), An Integrated PSA Approach to Independent Regulatory Evaluations of Nuclear Safety Assessments of Spanish Nuclear Power Stations, CSN publication CSN, 28.2002, Colección "Otros Documentos", 2002.

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

[11] USNRC, Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, LWR Edition, Reg. Guide 1.70, U.S. NRC, November 1978.

[12] USNRC, Standard Review Plan, NUREG-0800, Rev. 3, December 2015.

[13] ASME/ANS, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sb-2013, September 2013.

[14] USNRC, Severe Accident Risks. An assessment for five U.S. Nuclear Power Plants, NUREG 1150, 1989.

[15] IAEA, INSAG-6 Probabilistic Safety Assessment, Safety Series No. 75-INSAG-6, IAEA, 1992.

[16] USNRC, MELCOR Computer Code Manuals, NUREG/CR-6119, October, 2000.

[17] J.M. Griesmeyer, L.N. Smith, A Reference Manual for the Event Progression Analysis Code (EVNTRE), NUREG/CR-5174, SAND88-1607, Sandia National Laboratories, Albuquerque, NM, 1989.

[18] T. Aldemir 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, Kusadasi-Aydin, Turkey, August 24-28, 1992.

[19] T. Aldemir, A Survey of Dynamic Methodologies for Probabilistic Safety Assessment of Nuclear Power Plants, Annals of Nuclear Energy 52, 113–124, (2013).

[20] J. Devooght and C. Smidts, Probabilistic Reactor Dynamics (I). The Theory of Continuous Event Trees, Nucl. Sci. Eng. 111, 229-240, (1992).

[21] J. Devooght and C. Smidts., Probabilistic Reactor Dynamics (II). A Monte Carlo Study of a Fast Reactor Transient, Nucl. Sci. Eng. 111, 241-256, (1992).

[22] J. Devooght, J.M. Izquierdo and E. Meléndez, Relationships between Probabilistic Dynamics and Event Trees, Reliability Engineering & System Safety, 52 197-209, (1996).

[23] P.E. Labeau and J.M. Izquierdo, Modeling PSA problems (I). The Stimulus Driven Theory of Probabilistic Dynamics, Nuclear Science and Engineering, 150, 115–139, (2005).

[24] P.E. Labeau and J.M. Izquierdo, Modeling PSA problems (II). A Cell-to-Cell Transport Theory Approach, Nuclear Science and Engineering, 150, 115–139, (2005).

[25] J.M. Izquierdo and P.E. Labeau, The Stimulus-Driven Theory of Probabilistic Dynamics as Framework for Probabilistic Safety Assessment, PSAM-7/ESREL-04 Conference, Springer, Berlin, Germany, 2004.

[26] C. Ibañez and J.M. Izquierdo, Theory of Stimulated Dynamics, Proyecto APSRIT (CSN-UPM), Métodos Avanzados de APS para una Regulación Indepediente de Tecnología, APSRIT/IT-09/0911, September 2009.

[27] J.M. Izquierdo and I. Cañamón, 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.

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

[29] L. Ibañez 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.

[30] J.M. Izquierdo, S. Galushin and M. Sánchez, 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.

[31] J.M. Izquierdo, C. Paris and M. Sánchez, The Theory of Transmission Functions and its Application to Protection Engineering, submitted to publication at Process Safety and Environmental Protection (November 2015).

[32] M. Sánchez 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.

[33] G. Cojazzi, E. Meléndez, J.M. Izquierdo and M. Sánchez, 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.

[34] J.M. Izquierdo, J. Hortal, E. Meléndez and M. Sánchez, 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).

[35] J.M. Izquierdo and M. Sánchez, Application of the Integrated Safety Assessment Methodology to the Emergency Procedures of a SGTR of a PWR, Reliability Engineering & System Safety, 45 159-173, (1994).

[36] M. Sánchez and J. Melara, 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.

[37] J.M. Izquierdo, C. Queral, R. Herrero, J. Hortal, M. Sánchez, E. Meléndez and R. Muñoz, 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.

[38] A. Trillo, E. Meléndez, M. Sánchez, E. Mínguez, R. Muñoz and J.M. Izquierdo, Analysis of the Steam Generator Tube Rupture Initiating Event, 24 Meeting of the Spanish Nuclear Society, Valladolid 14-16 de October de 1998.

[39] R. Muñoz, E. Meléndez, J.M. Izquierdo, E. Mínguez and M. Sánchez, DENDROS: A Second Generation Scheduler for Dynamic Event Trees, M&C'99, Madrid, 1999.

[40] E. Meléndez, J.M. Izquierdo, M. Sánchez, J. Hortal and A. Pérez, Tree Simulation Techniques for Integrated Safety Assessment, CSNI Specialist Meeting on Simulators and Plant Analysers, Espoo, Finland, 1999.

[41] J. Gil et al., 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.

[42] J.M. Izquierdo et al., SCAIS (Simulation Code System for Integrated Safety Assessment): Current status and applications, ESREL 2008 and 17th SRA Europe. Valencia (Spain), September, 2008.

[43] R. Herrero, A Standardized Methodology for the Linkage of Computer Codes. Application to RELAP5/Mod3.2, NUREG/IA-0179, USNRC. Office of Nuclear Regulatory Research, March 2000.

[44] J.M. Izquierdo, J. Hortal, F. Pelayo, J. Pérez, J.M. Rey, I. Veci and M. Sánchez, TRETA: a General Simulation Program with Application to Transients in NPPs, XIII Meeting Spanish Nuclear Society, October 1987.

[45] J.M. Izquierdo et al., TRETA and TIZONA Fast Running Thermal-Hydraulic Codes, Annals of Nuclear Energy 34 (2007) 533–549.

[46] N. de los Santos, Risk Assessment Tool, Proyecto APSRIT (CSN/UPM), Métodos Avanzados de APS para una Regulación Independiente de la Tecnología, APSRIT/IT-01/0710 (ver. 1), Madrid, July 2010.

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

[48] L. 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.

[49] J. Montero, C. Queral, J. Rivas, J. González, Effects of RCP trip when recovering HPSI during LOCA in a Westinghouse PWR, Nuclear Engineering and Design 280 (2014) 389–403.

[50] Teigen J., Ness E., Flandelsby F., Computerizing operating procedures with COPMA-II: A disturbance procedure from paper to COPMA-II implementation, Enlarged Halden Programme Group Meeting. Storefjell, Norway, 7th -12th March, 1993. OECD Halden Reactor Project.

[51] Bisio R., Hulsund J.E. and Nilsen S., Brief Introduction to the COPMA-III Tool. Halden Reactor Project, Institute for Energy Technology, 2000.

[52] Hortal, J., Simulation of Opertaing Procedures as a Tool for NPP Procedures Verification. Enlarged Halden Programme Group Meeting, Löen, Norway, 19th -24th- May 1996.

[53] Expósito, A., et al., Development of a software tool for the analysis and verification of emergency operating procedures through the integrated simulation of plant and operator actions. Annals of Nuclear energy 35, 2008, 1340–1359.

[54] M. Dusic, M. Dutton, H. Glaeser, J. Herb, J. Hortal, R. Mendizábal and F. Pelayo, Combining Insights from Probabilistic and Deterministic Safety Analyses in Option 4 from the IAEA Specific Safety Guide SSG-2, Nuclear Technology, Vol. 188, p. 63-77, Oct. 2014, http://dx.doi.org/10.13182/NT13-16

[55] C. Queral et al., Verification of SAMGs in SBO Sequences with Seal LOCA. Multiple Damage Indicators, Annals of Nuclear Energy 98 (2016) 90–111, http://dx.doi.org/10.1016/j.anucene.2016.07.021.

[56] Mendizábal R., Contribución al Estudio de las Metodologías de Cálculo Realista con Incertidumbre (BEPU), dentro del Análisis Determinista de Seguridad de Plantas Nucleares, Tesis Doctoral, Escuela Técnica Superior de Ingenieros Aeronáuticos, Universidad Politécnica de Madrid, 2016.

[57] M. Zancada, Consolidación del Acoplamiento entre un Código de Simulación Dinámica de Escenarios de Combustión de H2 en la Contención y Prototipo de Plataforma Computacional para APS de Centrales Nucleares, Thesis for the degree of Industrial Engineer, UPM, Madrid, November 2012.

[58] L.M. Gamo, Modernización del Prototipo de Código de Resolución de las Ecuaciones de TSD (Theory of Stimulated Dynamics) de Fiabilidad Dinámica y del Código GASTEMP de Simulación de Secuencias, Proyecto APSRIT (UPM-CSN) de Métodos Avanzados de APS para una Regulación Indepediente de Tecnología, APSRIT/IT-13/0712, (ver 1), Madrid, July 2012.

[59] A. Flores, J.M. Izquierdo, K. Tucek, E. Gallego, 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.

[60] A. Flores, J.M. Izquierdo, M. Sánchez, E. Gallego, Development of an Adequate Model for Verification of Design Safety-Margins of the HTTR Nuclear Test Facility", Progress in Nuclear Energy, 2012; pp. 1-2. ISSN 0149-1970, 2012.

[61] J. Yaochy, Surrogate-assisted evolutionary computation: Recent advances and future challenges, Sworm and Evolutionary computation 1(2011)61-70.

[62] Akcasu Z., Lellouche G. and Shotkin L., Mathematical methods in nuclear reactor dynamics, Published by Academic Press(1971), ISBN 10: 012047150, ISBN 13: 9780120471508.

[63] E. Zio, Integrated Deterministic and Probabilistic Safety Assessment: Concepts, Challenges, Research Directions, Nuclear Engineering and Design 280, 413–419, 2014.

[64] INTECH, Fourier Transform Applications. Chapter 12: Hilbert Transform and Applications, Edited by Salih Mohammed Salih, ISBN 978-953-51-0518-3, 312 pages, DOI: 10.5772/2658.

[65] N. Vu Truong, Nonlinear System Identification Using Wavelet based SDP Models, PhD Dissertation, School of Electrical and Computer Engineering, RMIT University, April 2008.

[66] Izquierdo J.M., Hortal F.J., Vanhoenacker L., Merits and Limits of Thermalhydraulic Plant Simulations. Towards a Unified Approach to Qualify Plant Models, Nuclear Engineering and Design, 145, pp. 175-205, 1993.

[67] 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.

[68] J.A. Gieseke et al., Source Term Code Package: A User's Guide, NUREG/CR-4587, BMI-2138, Battelle Columbus Division, Columbus, OH, July 1986.

[69] J.M. Izquierdo et al., Evaluación del Análisis de APS- Nivel 2 de la C.N. de Ascó. Proyecto MOSI de asimilación de la metodología ERI para el APS de nivel 2 de centrales españolas. Centrales españolas PWR Westinghouse tres lazos representadas por C.N. Ascó. Resumen y Conclusiones, CSN, 2001, CSN/IEV/MOSI/ASO/0101/72.

[70] D. Mandelli, T. Aldemir and A. Yilmaz and, Scenario Aggregation in Dynamic PRA Uncertainty Quantification, ICAPP'10, CD-ROM, American Nuclear Society, LaGrange Park, IL (2010).

[71] D. Mandelli, A. Yilmaz, T. Aldemir, K. Metzroh and R. Denning, Scenario Clustering and Dynamic Probabilistic Risk Assessment, Reliab. Engng & System Safety, 115, 146-160 (2013).

The importance of accident time evolution in regulatory safety assessment. Independent, quantitative tools and methods at CSN to ensure adequate PSA/DSA applications. Deterministic Aspects

Colección
Otros Documentos CSN

CSN CONSEJO DE SEGURIDAD NUCLEAR