An integrated PSA approach to independent regulatory evaluations of nuclear safety assessments of Spanish nuclear power stations

CSN

Colección
Otros Documentos
28.2002

CSN

CONSEJO DE
SEGURIDAD NUCLEAR

An integrated PSA approach to independent regulatory evaluations of nuclear safety assessments of Spanish nuclear power stations

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

CSN CONSEJO DE SEGURIDAD NUCLEAR

Colección
Otros Documentos CSN
Referencia: ODE-04.18

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

Imprime: Fareso, S. A.
Depósito Legal: M. 49.266-2002

Contents

Resumen y presentación

Resumen y presentación

Este documento revisa[1] el trabajo realizado en el Consejo de Seguridad Nuclear para consolidar un enfoque integrado de los análisis probabilistas de seguridad (APS), implantado en un entorno de simulación matemática vía códigos de cálculo, para la evaluación independiente de los APS realizados por la industria nuclear española. En él se desarrollan los siguientes puntos:

- Una breve introducción a la situación del trabajo realizado anteriormente a 1992. El esfuerzo se dedicó a estudios independientes con el objetivo de entender los métodos y prácticas para evaluar las conclusiones de los APS españoles. Se mencionan de pasada los fundamentos y el marco científico que ha guiado la línea de trabajo.

- Principales características de desarrollos antiguos y modernos para sintetizar un paquete integrado de simulación capaz de verificar y/o reproducir partes de un APS con objetivo de evaluación reguladora.

- Pasos dados en el desarrollo de una nueva metodología integrada (Integrated Safety Assessment) y un paquete software asociado, utilizado en la actualidad por el Área de Simulación y Modelación (MOSI) en el CSN. En cada paso de tiempo se pueden acoplar:

  - la simulación de árboles de evoluciones temporales de secuencias de accidentes nucleares, resultado de explorar las degradaciones potenciales de los equipos, consecuencia de la ocurrencia de sucesos iniciadores
  - los cálculos de la probabilidad de las secuencias, y
  - la simulación de las acciones de operador

- Extensiones recientes. Nuevas contribuciones que completan un enfoque científico coherente de los análisis probabilistas de seguridad de las centrales nucleares.

Aunque escrito por cuatro de los miembros de la actual Área MOSI, esta revisión cubre un período mucho más extenso, que incluyó actividades de las unidades organizativas del CSN que precedieron a MOSI. Es por tanto resultado del trabajo de muchas personas, algunos de ellos trabajando temporalmente, otros de manera más permanente. De entre todos ellos hay que destacar a Rafael Mendizábal, Fernando Pelayo, Julio Pérez y José María Rey que tanto contribuyeron al desarrollo del sistema de simulación.

La lista de contribuyentes adicionales sería seguramente incompleta y muy numerosa. Hemos preferido incluir una lista detallada de referencias en la sección de perspectiva histórica

[1] La referencia [1] es una versión reducida de este documento.

como la mejor manera de reconocer su trabajo. Ciertamente todas estas referencias no tienen la misma importancia, pero en su conjunto han resultado pasos esenciales.

Pedimos perdón por escribirlo en un pobre inglés. Un propósito importante ha sido que sirviera de vehículo de comunicación con la comunidad internacional. Desgraciadamente tenemos demasiado pocos recursos para permitirnos el esfuerzo de preparar dos versiones, y son todavía demasiado pocos los que se dedican en España a este mundo particularmente difícil de la interfase entre la fiabilidad de los sistemas y la evolución dinámica de los accidentes en los estudios de APS. Difícil sí, pero esencial a la evaluación de la seguridad. Esperamos que este trabajo contribuya a un mejor entendimiento mutuo entre los técnicos del CSN y de fuera de él.

Summary and presentation

Summary and presentation

This document surveys[2] the work made at CSN to establish an integrated PSA approach implemented in a mathematical and code simulation framework for independent assessment of safety studies. It will elaborate on the following points:

- A brief introduction on the situation of the work performed prior to 1992. The effort was devoted to independent studies made to understand the practice and methods to evaluate Probabilistic Safety Assessment (PSA) conclusions of Spanish Nuclear Power Plants. It will touch upon the theoretical framework that guided the approach.

- Main features of old and new developments to synthesize a simulation package able to independently verify and/or reproduce portions of a PSA with the aim of its regulatory evaluation.

- Steps done in the development of the Integrated Safety Assessment (ISA) software package and methodology used at present by the Area of Modeling and Simulation (MOSI) at CSN. At each time step, the following can be coupled:

  i) the simulation of trees of accident sequences evolutions, result of exploring potential equipment degradations under initiating events,
  ii) the sequence probability calculations and
  iii) the simulation of operator actions.

- Recent extensions. New contributions that complete the picture of a coherent scientific approach for Probabilistic Risk Assessment of Nuclear Power Plants.

Although written by four members of todays MOSI, it covers a much extended period that included activities of the CSN organizational units that preceded MOSI. This means the work of many people, some of them working part time, some on a more permanent basis. We are proud of mentioning among them Rafael Mendizábal, Fernando Pelayo, Julio Pérez and José María Rey that so much contributed to the development of the simulation framework.

The list of additional contributors would be surely incomplete and too numerous. So, we have included a detailed list of references in the historic perspective section as the best way to recognize them. Certainly not all of these references are of the same importance, but, taken together, they were necessary steps.

[2] For a short version of this report see reference [1].

We apologize for writing it in poor English. A major purpose has been for the document to serve as a vehicle of communication with the international community. Unfortunately we have too scarce resources as to spend time in two versions, and there are still too few people in Spain working in this particularly difficult world of the interaction of system reliability and the course of accidents in PSAs. Difficult, but essential to safety assessment. We hope this report can contribute to a better mutual technical understanding inside and outside of CSN.

I. Historic perspective

I. Historic perspective

In 1974, the Nuclear Research Centre of Madrid (JEN) [2,3] started the painful work of fast assimilation of transient and accident analysis of Nuclear Power Plants. It included the methods used by the then already mature nuclear industry to ensure safety of the Spanish nuclear plants that were under licensing at that time. The major problem was to understand the overall approach through the many fragments of information available.

All the way to 1990, and after the creation of the CSN, we developed a conceptual frame [3,4,5] that summarised our successive experience in licensing of transient analysis (Chapter 15 of the Safety Analysis Reports (SAR))[6,7,8,9,10,11], Start-up Testing [12,13,14,15], Nuclear Operations [16,17,18] as well as licensing of the operating crews of our PWR Plants. We generated methodologies [19,20,21,22] and software packages [16,23,24,25,26,27,28,29,30] that implemented the conceptual frame and provided great help to our licensing work in the practical arena.

We took a view of SAR transient analysis as the legal proof that the optimized design of nuclear plant protection systems fulfils regulatory risk criteria. However, we soon discovered the need to go deeper in order to address the following two main aspects of the problem:

- Automatic protective intervention decision making through reactor trip and safeguard system setpoints and signal processing. These are described in plant documents, for instance the "Precautions, Limitations and Set-points" of Westinghouse Plants.

- Manual protective intervention decision making as stated in the Technical Specifications for Operation and Fault and Emergency Instructions. This last aspect of the problem was hard to incorporate because of the emphasis in the design of automatic systems of the main stream of the licensing practice, at least prior to the occurrence of the TMI accident.

This experience, together with the increasing trend towards risk informed regulation shifted our focus on strict PSA issues. Correct versus incorrect event tree delineation was the heart of the difficulty. We as regulators have tried to focus on this point because of its qualitative, essential impact on the results, point not covered by uncertainty analysis.

Since 1992, new international developments, including the theory of Probabilistic Dynamics [31,32,33,34], formalised an abstract but rigorous approach that clearly covered some of the more important aspects of our frame. Although Probabilistic Dynamics was clearly a proper framework it was too general to be applied directly and it was necessary a specific approach for PSA implementation. Thus, the heart of present activity is to adapt these general ideas to converge with present engineering practice. This is the case of our ISA development and its recent extensions [19,20,35,36, 42,43,44,45,46,48,51,80].

II. Modeling and simulation view of current PSA practice and the safety assessment work by the regulatory body

II. Modeling and simulation view of current PSA practice and the safety assessment work by the regulatory body

II.1. Protection Engineering and PSA. The role of modeling and simulation

For the purposes of this review, we understand by Protection Engineering, [1,3] the set of disciplines, methods and technologies that deal with the design and optimization of protective measures, both manual and automatic, in (usually large) industrial facilities. The optimization is constrained by acceptance criteria derived from general public risk limit regulations, as described for instance by risk limit curves (see below).

We denote generically as facility protection the set of systems, system features, and safety oriented decision-making processes whose objective is to optimize plant response with respect to damage under any credible event. Regulations and regulatory bodies should ensure that the facility protection prevents undue public risk against any credible event. Note the enveloping character of the analysis, which makes Protection Engineering assessment so complex and singular. Assessing damage for a few particular events is of little regulatory interest. What counts is to prove that under no credible circumstance can damage indicators go over unacceptable limits. These limits are inherently probabilistic in nature, since they are functions of the frequency as it will be later explained.

Computer modeling, understood as the process to make precise statements and translate ideas into computer language, provides a rigorous framework for simulation to explicitly represent the impact of both protective measures and decisions for their interventions during the time evolution of accident scenarios. The results of the simulation and the defence of its underlying safety case allow for a traceable procedure for compliance with risk curves acceptance criteria. As a result, PSA may be viewed as a computer aided protection-engineering methodology, based on simulation. As of today, a substantial body of theory, in rapid evolution during the last decade, is providing a sound scientific basis and identifying improvement areas as well. We use to call it Protection Theory, by analogy with Control Theory[2]. However, this conception extends the usual scope of PSA as currently understood, and integrates the regulatory evaluation of the deterministic transient analysis. It is in this broad and integrated sense that our PSA approach is used.

II.2. Problem Description. Key issues and requirements

The basic problem is how to optimize the protection of a complex facility such as a Nuclear Power Plant. Optimization is needed in order to assure intervention if necessary and prevent it if

[2] Control theory specialists are also starting to discuss similar issues [37,38]

unnecessary; a requirement derived from the often-aggressive nature of the safety measures. Decision for interventions ought to be automatic in the short term after an accident and concurrently, and interactively manual, soon after. Time scales vary from seconds to days or even months and very complicated phenomena may appear as a result of the interaction between the plant and the automatic systems. It paves the way for scenarios that easily escape individual's mind capability to predict behavior and requires carefully planned emergency instructions.

The need of decision making, automatic and manual, forced to be fast, reliable, feasible, concrete and complete, poses very serious challenges for analysis. While a de-coupled treatment of different aspects is inevitable to simplify and structure at different stages, it makes room for possible holes in the overall approach. For example, as the TMI accident showed, magnifying an initiator, say a large LOCA, as a way to design enveloping protections does not lead necessarily to an optimal protection because milder events, say a small LOCA, may then go inadvertent to the protection detectors. Verification of this enveloping character of the design is a major objective of safety assessment.

The design of envelopes cannot be avoided, due to the infinity of possible events, and to ensure the completeness of the spectrum of selected design basis scenarios becomes a touchy and subtle analysis problem. In all cases simulation is required due to obvious limitations to test protections with real accidents.

Nuclear applications are today concentrated in PSA studies. The typical setup of the problem assumes a given initial steady state (including different status and configurations of key active and standby systems) of a nuclear facility, that experiences an initial stochastic failure and induces a time evolution followed by subsequent conditioned events. The overall time window is broken-up by the potential occurrence of core melting and/or reactor coolant boundary failure or containment bypass (PSA level I). If such is the case, PSA level II covers the potential for large radiological sources outside containment. It is essential to bound the compound frequency of the different sequences that may generate damage in excess of a given value (exceedance curves). Damage is indicated by some combinations of process variables, eventually associated to a threshold value below which there is no real damage. Typical damage indicators are core melt correlations, fission product concentrations or released radiological activity.

The problem is usually subdivided by progression intervals that describe the efficiency of the different protection interventions to cope with the sequential appearance of degradation phenomena. Unsuccessful scenarios are precursors[3] for the next phase that filter out the ones where the protection was already satisfactory. For instance, the typical setup of the problem in PSA-2,

[3] See comments in section 3.2

assumes a given PSA-1 set of risk sequences, leading to core damage, that act as precursors of a further time evolution that may challenge the containment and/or generate the potential for a source term to the outside.

The analysis may be oriented to

- Identification of vulnerabilities (mainly regarding design features and systems) without taking any substantial accident management action within a pre-established time window (typically 48 hours after accident occurrence). Bounds to the amount of damage and source terms during this period are quantified, without pretending to arrest the accident. In this case PSA techniques may also indicate qualitatively the relative efficiency of proposed mitigation measures. The analysis also provides information for emergency planning.

- Assessment of capability for accident progression arrest, accounting for management actions. As for any success state, a final state not adding further damage is expected. In this case PSA-2 techniques may be used to confirm adequacy of the detailed emergency guidelines.

In principle, those aspects may be contemplated at any of the progression intervals, verifying the adequacy of different aspects of the envisaged protections.

II.3. Regulatory framework. Establishing unacceptable damage. Unified view of deterministic (protection design) and probabilistic (risk verification) analysis

There are many analogies and some differences between the usual deterministic and probabilistic approaches, two faces of the same coin. The main reason for the similarities is apparent when comparing event trees and design basis transients. Both are representations of the evolution that follows an initiating event, and in both cases a frequency is assigned to the initiating event. Both of them are risk-enveloping representatives of groups of evolutions with common characteristics. Also, the design basis transients can be viewed as particular sequences in a complete set of event trees. From a regulatory perspective the differences are mainly related with the region of the risk curves where both types of analysis are applied, as seen in figure 1 below. The risk curves may be understood by assuming that a complete partition of the space of facility transients has been done with the aid of a set of event trees. This results in a set of sequences that include, as particular cases, the design basis transients.

The risk curves represent estimated/acceptable frequency of exceedance of an amount of damage. The risk limit, identified in figure 1 as "damage limit", represents regulatory requirements established on selected damage variables with technical, social and environmental criteria. The nature of the selected variables and shape of the curves have a deep basis that can not be discussed here (see [39] for details).

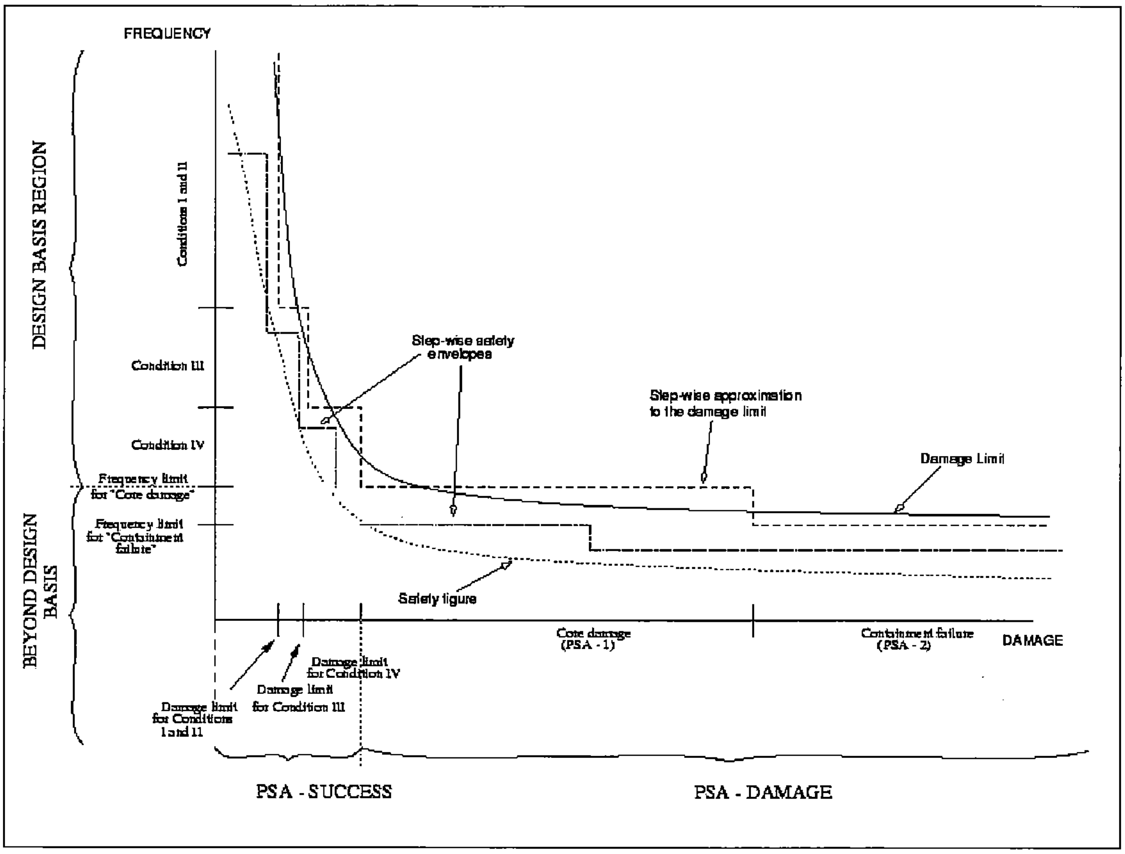

Figure 1. The regulatory risk curve showing the PSA versus the design regions

The actual risk curve of the facility, identified as "plant safety picture" in the figure, can be estimated by adding-up the frequency of all the sequences generating damage in excess of each damage value.

The "distance" between both curves is a good representation of the safety margin available and allows judgement of the impact of any facility change into public safety.

In most cases, the risk limit curve is replaced by a step-wise approximation (see figure 1), that enables us to qualitatively describe the focus and objectives of deterministic and probabilistic analyses. Its projection on the vertical axis defines the frequency ranges of "design basis" (divided in design frequency conditions) and "beyond design basis" transients. For each condition, represented by a rather wide interval in the "design basis" region there is a well-defined damage limit. On the other hand, the projection on the horizontal axis defines the ranges of PSA-success and PSA-damage; the latter divided according to the PSA levels. For each PSA level, there is a well-defined frequency limit.

The major difference is then that classical PSA is mainly oriented towards lower frequency sequences that occur as a result of circumstances "beyond the design basis", while the deterministic analysis is oriented towards higher frequency. As indicated in the figure, damage should be discriminated more in the deterministic case, while frequency should be more precisely evaluated in the PSA region.

The complementarity of the regions of application does not imply independence of methodologies. Important interactions between them have been identified [39] and any evaluation of licensing issues supported by a safety analysis must consider both aspects of the problem. Even if the problem is clearly located in the "design basis region", i.e., it is supported by a deterministic analysis, there should be a check of the assumptions and inputs of the probabilistic analysis. The same is true in the opposite way: any licensing issue supported by a probabilistic analysis must include a check of the validity of potentially affected assumptions of the deterministic analysis.

This conception of the safety analysis provides the fundamentals to implement the principles driving the risk-informed regulation that is today the subject of great regulatory attention worldwide. Integrated methods and tools can also be designed to address the safety problem as a whole, including both the "deterministic" and "probabilistic" issues.

II.4. Basic features and difficulties of PSA-1 and PSA-2 from the modeling and simulation perspective

PSA-1

An important number of the paths of a PSA-1 system event tree results from automatic or human decisions about system interventions. Both types of decisions are conditioned by set points that trigger either the initiation of automatic systems or control room alarms. A key point is to explore the possible combinations in case of failures of the underlying safety systems. As a consequence of the number of headers and branching points, as well as the consideration of human actions, the complexity of the resultant dynamics makes very difficult to ascertain the actual activation of alarms or set points. Important implicit assumptions, difficult to assess, are inherent in the design of event trees. In addition, human actions involve psychological factors proved to be significant and influenced by the dynamics of the context.

On the other hand, due to the level of detail of the boolean model required in present day PSA models, the frequency estimate is associated with the handling of large fault trees and the size of this aspect of the problem is quite formidable. Powerful software is already developed. However, the large size, together with the increase in the number of headers, (i.e. increase of the number of boolean intersections of large fault trees) places the computational effort to quantify the sequences of the tree close to computer limits. It is also worth mentioning that probabilities of basic events are time dependent with two widely different time scales, maintenance of equipment in one side and the time scale of the accident on the other. Finally, boundary conditions for fault trees are also dependent on the dynamics [40] and its implementation in the boolean model also implies dynamic assumptions.

PSA-2

PSA-2 considers protection assessment of a nuclear power plant when we assume the possibility of core damage, a possibility necessary to be contemplated after the occurrence of accidents like TMI or Chernobyl. Adequate protection is needed in order to "identify and correct potential plant vulnerabilities and ensure enough and positive protective intervention measures" to avoid radioactive releases to the environment.

PSA-2 applies to the high damage-low frequency risk region, where the estimation of the frequency should be made more precise than the estimate of its corresponding damage. Priority is given to ruling out non-credible events and distinguish them from credible but of very low frequency. On the other hand, a precise estimate of damage is precluded by the uncertainty about phenomena. We cannot be sure now that, if the system reaches certain regions of the process variables, a given phenomenon will occur. Rather, we only know that it has a higher or lower probability of occurrence. Should it occur, our information about its physics may be substandard. In addition, the many possibilities of prior to core damage scenarios are to be accounted for, as filtered by PSA level-1 studies.

In event tree terms, all this translates into a large number of headers, new ones accounting for phenomena. This "phenomena" addition to the "systems event tree" is typically called the APET (Accident Progression Event Tree). Again, the assurance of the enveloping character of the analysis is the big challenge.

Modeling phenomena, once they occur, is often made by means of "parameters" that replace unknown functions of dynamic variables. These models incorporate known information and at the same time reflect, through the parameter range values, the parametric uncertainty band. Comparison with the so called mechanistic models allows to ascertain the degree of representativity of the parametric models and its parameter functional dependence. Thus, in PSA-2 there is more dependence on dynamics.

Finally, human actions under severe scenarios are organized such that they also involve "out of control room" decision making [41]. The need has been created to develop appropriate procedures for technical support centers. The simulation of this type of procedures to verify its acceptability opens new areas in the domain of procedure computerization [42,73] and interaction with the dynamics of uncertain scenarios.

For these and other reasons, room for improvement is today recognized in the modeling of dynamic effects and its influence in a PSA study. These improvements would alleviate the regulatory verification of PSA completeness and consistency, particularly event tree delineation. All these difficulties are the main frame that justifies the developments described below.

III. CSN developments for independent verification of event tree delineation

III. CSN developments for independent verification of event tree delineation

III.1. ISA: Integrated sequence assessment methodology and simulation software

As above indicated, event tree delineation is a critical point in the evaluation of a given PSA. The designer task is very complex and to correctly delineate a tree can be considered an art. The regulatory task is in a sense simpler as it reduces to check the validity of a given proposal. Within CSN, we have developed verification methods [43,44,45] through the years.

A set of acceptance criteria was derived from the very definition of an event tree, and from the theoretical approach that is at the basis of the method. They imply about ten checks that should be satisfied by the proposed solutions. In order to assess a proposed event tree, an automatically simulated event tree sequence sampling is performed using the same initiator and the same "as proposed" headers with the software package described below. The method has been referred to in previous publications as Integrated Safety Assessment (ISA). Since the acronym and the concept are similar to the Integrated Sequence Analysis considered by others [46], both denominations can be used. More details are given below.

The ISA methodology [19,20] is a systematic approach to verify a pre-specified set of risk requirements characterized by imposed sequence damage limits, D_l^L which are decreasing functions of the sequence frequency. It can be viewed as a dynamic extension of PSA, based on the automatic generation of Dynamic Event Trees (DET). Of particular interest is the case of system state transitions which are conditioned by deterministic events given by the dynamic evolution (set point transitions), which give rise to the concept of Deterministic Dynamic Event Tree (DDET) [20].

Operator actions are also conditioned by dynamic events (alarms) but their execution occurs at a random time within a time window after the conditioning event. This kind of transitions, that we call operator transitions, can also be included in the scope of the method, as briefly described in the section on extensions below.

III.1.1. Theoretical basis

Basic concepts and principles supporting ISA were established during a co-operative work developed by the Université Libre de Bruxelles (ULB) and CSN [20]. The formalization of the method was afforded with the aid of the Theory of Probabilistic Dynamics [27,32], which deals with the evolution of dynamic systems subject to discrete events that alter the dynamic behavior and whose probability depends on the dynamic evolution.

In general, the system dynamics is described by equations of the type:

$$\vec{x} = \vec{g}_{\vec{j}}(\vec{u},t) \tag{1}$$

where $\vec{x}$ is the vector of process variables or dynamic state, $\vec{u}$ is the vector of initial conditions, $\vec{j}$ is the vector of system configuration or logical state and t is time. The dynamic and logical states, considered together, describe the so-called combined state of the system. Damage will be represented by damage variables D_l, which are functions of the dynamic state $\vec{x}$. In practice, the evolution is obtained with continuous thermalhydraulic simulations.

Events consist of transitions of the logical state that, in general, will change the dynamic equations, i.e., the dynamic system behavior.

The probability π of being at a combined state ($\vec{x}$, $\vec{j}$) at time t is governed by balance equations of the form:

$$\frac{D}{Dt}\pi_{\vec{j}}(\vec{x},t) = -\lambda_{\vec{j}}(\vec{x})\pi_{\vec{j}}(\vec{x},t) + \xi_{\vec{j}}(\vec{x},t) \tag{2}$$

where $\frac{D\bullet}{Dt} \equiv \frac{\partial\bullet}{\partial t} + div\left(\frac{d\vec{x}}{dt}\bullet\right)$ is the transport operator,

$\lambda_{\vec{j}}(\vec{x}) \equiv \sum_{k \neq j} p_{\vec{j}\to\vec{k}}(\vec{x})$ is the transition rate from state $\vec{j}$ to any other logical state and

$\xi_{\vec{j}}(\vec{x},t) \equiv \sum_{k \neq j} p_{\vec{k}\to\vec{j}}(\vec{x})\pi_{\vec{k}}(\vec{x},t)$ is the transition rate from any other state into state $\vec{j}$.

Solving equation (2) with initial condition π^0_α and with the condition that transitions are deterministically conditioned by set points (i.e., they only can occur at the time the set point is reached), we obtain the expression for the probability of being at logical state $\vec{j}$, for any dynamic state $\vec{x}$:

$$\pi_{\vec{j}}(t) \equiv \int \pi_{\vec{j}}(\vec{x},t)d\vec{x} = \pi^0_\alpha X_{\alpha\vec{j}_0}(\vec{x}_0)\sum_{n=0}^{\infty}\sum_{Path_n}\theta(t-\tau_n)\prod_{l=0}^{n} X_{j_l j_{l+1}}(\vec{u}_s^{\,l+1}) \tag{3}$$

π^0_α is the probability of the initial state and $X_{\alpha\vec{j}_0}(\vec{x}_0)$ is the probability of the initiating event. The index $Path_n$ indicates any sequence of n transitions starting at state $\vec{j}_0$ and finishing at state $\vec{j}$ and τ_n indicates the time of the n-th transition.

Each non-zero term in the right-hand side of equation (3) contributes exactly in the same way as each associated sequence in an equivalent static event tree. However, the determination of the contributing path is controlled by the step functions θ, switching at times τ_n, i.e., when the initiation criteria are reached. This way, the influence of protection set points is taken into account. Equation (3) describes a Deterministic Dynamic Event Tree and is the main support of the ISA methodology [20].

The system failure probabilities that compose the product on the right-hand side of equation (3) are also varying in time. However, there are two points that should be taken into account. First, they refer to standby systems and, therefore, failure probabilities are not likely to depend on system dynamics. Second, the time scale of probability variation is much larger than the system accident time scale. The consequence of the first point is that equation (3) reduces to a classical Markov system or to the classical boolean intersection of the large front line systems fault trees, typical of PSA-1. Probability calculations then become decoupled from dynamic events and, therefore, from damage calculations. The second point allows considering that failure probabilities do not change during the accident sequence and their value may be computed, in the large time scale, at the time of the initiating event. Extensions to this approach allowing for a stochastic delay in the transitions are now under research [47].

III.1.2. Software package

The application of ISA, requires a set of computational tools [48], as shown in the self-explanatory Figure 2, allowing for automatic generation of Deterministic Dynamic Event Trees. The set has been applied to some examples [36,43,44,45,49] that have proved its usability.

It includes:

- ***Event scheduler***. The functions of the event scheduler in the example cases were initially performed by DYLAM [50], a code developed at the JRC Ispra for this purpose. A new scheduler [51], better adapted to the ISA methodology has now been developed that entirely replaces DYLAM. It improves the modularity of the overall system and the parallelisation of the event tree generation.

- ***The plant model*** is fully operative and adapted to perform tree simulations under control of the scheduler. For PSA-1 applications there are three versions of the plant simulator. TRETA for PWR plants, TIZONA [26,29,30,52,53,54] for BWR plants and BABIECA for general-

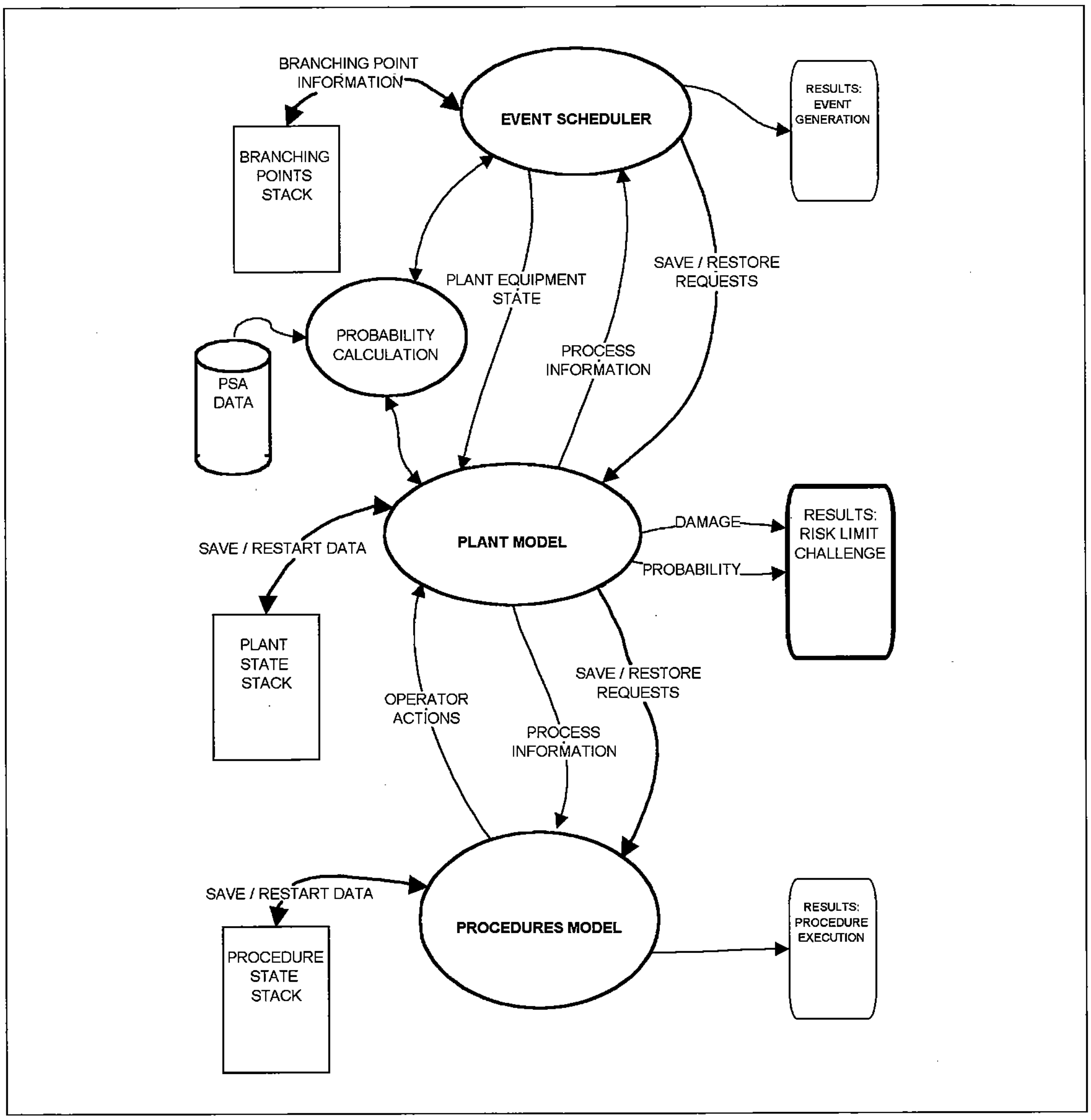

Figure 2. Basic elements of the ISA software package

purpose simulations, including non-nuclear technologies. In addition to its own simulation capabilities, the plant simulator provides means to extend the application scope by using external codes as simulation modules when needed. For example, both TIZONA and TRETA have been coupled with simplified severe accident models to simulate accident scenarios going beyond the design basis assumptions. For PSA-2 applications we have linked to the set the MAAP code, and we are currently incorporating MELCOR modules as well.

All those codes are used for the purpose of verifying the completeness of the tree. Once a given sequence is identified as conflictive from a safety standpoint, it is reproduced off-line with full scope plant models. At present we use RELAP5 [56,57,58,59] and MELCOR [section 5.4 of ref. 87] respectively for this purpose. We are currently working in parallel in the Consolidated Thermalhydraulic Code USNRC programs [60,61,62,63,64] to replace those with the consolidated versions. These versions contain features that allow direct connection to the rest of the system [65,71].

In-depth post-processing techniques [66,67,68,69,70,71,72], developed to ensure correct results of the large code plant model runs, also provide a method to consistently feed the simplified models.

- *Emergency procedures and HRA simulation.* Two ways to model procedures have been considered. A prototype called HOI has been used for those examples where the generation of the DDET was fully automatic [43,44,45]. For future applications, COPMA-II, a computerized procedure system developed at the Halden Reactor Project for operator support, is being adapted for simulation [73]. The system has been already used for interactively controlled simulation. The human factors and HRA models have not been included in the ISA system used at CSN. However, PSA studies include human factors and HRA analyses that are being considered in the framework of the methodology. The intended purpose is to provide capability, at least, to assess the HRA analysis included in real PSA [40].

- *Probability calculations.* They have been performed off-line in the application examples. The minimal cut sets representation of system fault trees, which is the format used in the PSA study, is not adequate for fast on-line probability computation. Alternative algorithms based on the representation of fault trees using the Binary Decision Diagrams (BDD) formalism are being implemented in a new computational module. Auxiliary programs, as for example RiskSpectrum [76] are also being used or developed to convert the minimal cut set representation into BDD format.

III.2. SGTR as example of evaluation of event trees in Spanish plants

A full scale application of this integrated software package to the independent verification of the event tree delineation and computation of the steam generator tube rupture initiating event of a Spanish PWR plant has been completed at CSN during 1999. The study was preceded by a precursor analysis to filter out success sequences. As part of the study, ten acceptance criteria for correct event trees were defined, rigorously derived from the very concept of what an event tree means. A number of inconsistencies were found in the utility delineation, made with classical techniques at high quality level. The inconsistencies were related with details of the emergency procedures when combined with the complex dynamics involved and the large number of branches. This is an indication that delineation of event trees is very difficult unless proper simulation of the branches and operator actions is done, a task that calls for integrated tree simulation.

Precursor study[4]

A progression interval was chosen characterized by the loss of subcooling margin, a necessary, but insufficient condition for core damage. It can be considered a PSA level zero analysis. The software package generated tree simulation results like those in figure 3 where success and failure sequence branches are numbered according to the status of important valves and pumps. The detailed evolution of the subcooling margin is represented in response to the execution of emergency procedure steps, also numbered in the right vertical axis.

This precursor study identified sequences with reactor coolant pump trip as candidates apparently overlooked in the industry reference study. Most of them were a consequence of the details of the procedures involved.

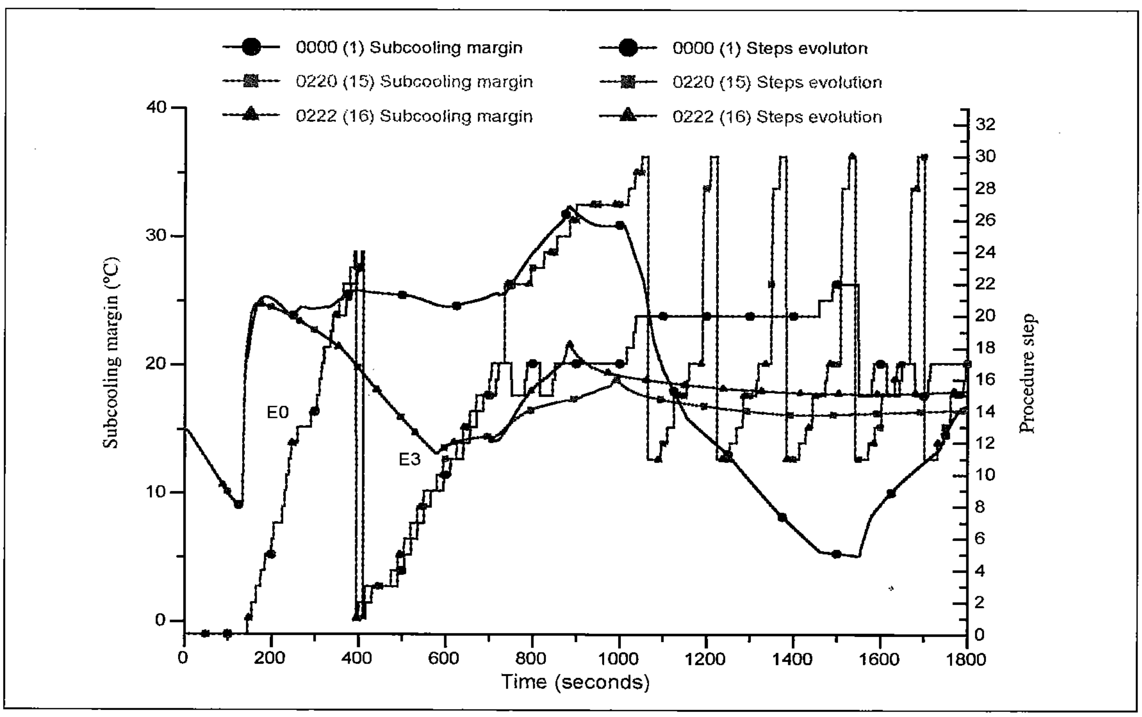

Figure 3. SGTR-ISA precursor study. Subcooling margin event tree simulation results

[4] In the sequel, the term "Precursor Study" refers to a broader concept than the traditional Precursor Analysis used to indicate a Probabilistic Incident Analysis. In general, we call "Precursor Study" to any analysis on the relationships between subsequent progression intervals.

Table 1. Features of the SGTR event tree study

Scoping study with automatic techniques:
Tree simulation capability Emergency Procedures Dynamics: TRETA/MAAP/HOI/BDDs 150 TRETA/MAAP calculations Boolean: RISKSPECTRUM pre-processing of BDD's
Detailed study for significant sequences
Complex TH codes Explore safety issues 36 RELAP5 calculations Feedback to scoping analysis Doubts about results resolved with post-processing

Event tree results

Once the candidate precursor sequences were identified, they were taken as equivalent initiators of the event tree for core damage. Prompt versus delayed core damage mechanisms and corresponding damage variables were identified. They gave rise to different PSA subproblems each one generating a partial event tree. Candidate failure sequences involving deep thermalhydraulic mechanisms were revisited with RELAP5. Some features of the study are summarized in table 1.

From the many results obtained, we select in figure 4 some of the identified sequences, 2, 6, 13, where disagreement with the reference industry case was found. The following illustrates the type of conclusions obtained:

- Sequences 2 and 6: The header relative to the control of the safety injection system (HPIS), should include the manual action of tripping one of the HPIS pumps (steps 18.d and 50.c of the emergency instruction). MAAP results showed that with two pumps, the set point of the secondary safety valves was exceeded, resulting in a loss of water of feeding storage tanks and ultimate HPIS loss. As a result, acceptance criterion 7 relative to the enveloping character of those sequences is violated unless the identified action is taken.

- Sequence 13: RELAP5 calculations show that after the feed and bleed operation, as requested by the emergency procedure, the primary coolant system portion where the hot leg temperature sensors are located, stays vaporized and at high temperature, while the core is maintained cooled. As a result, headers representing the operator actions for safety injection control and residual heat removal mitigation are not activated, violating acceptance criterion 3.

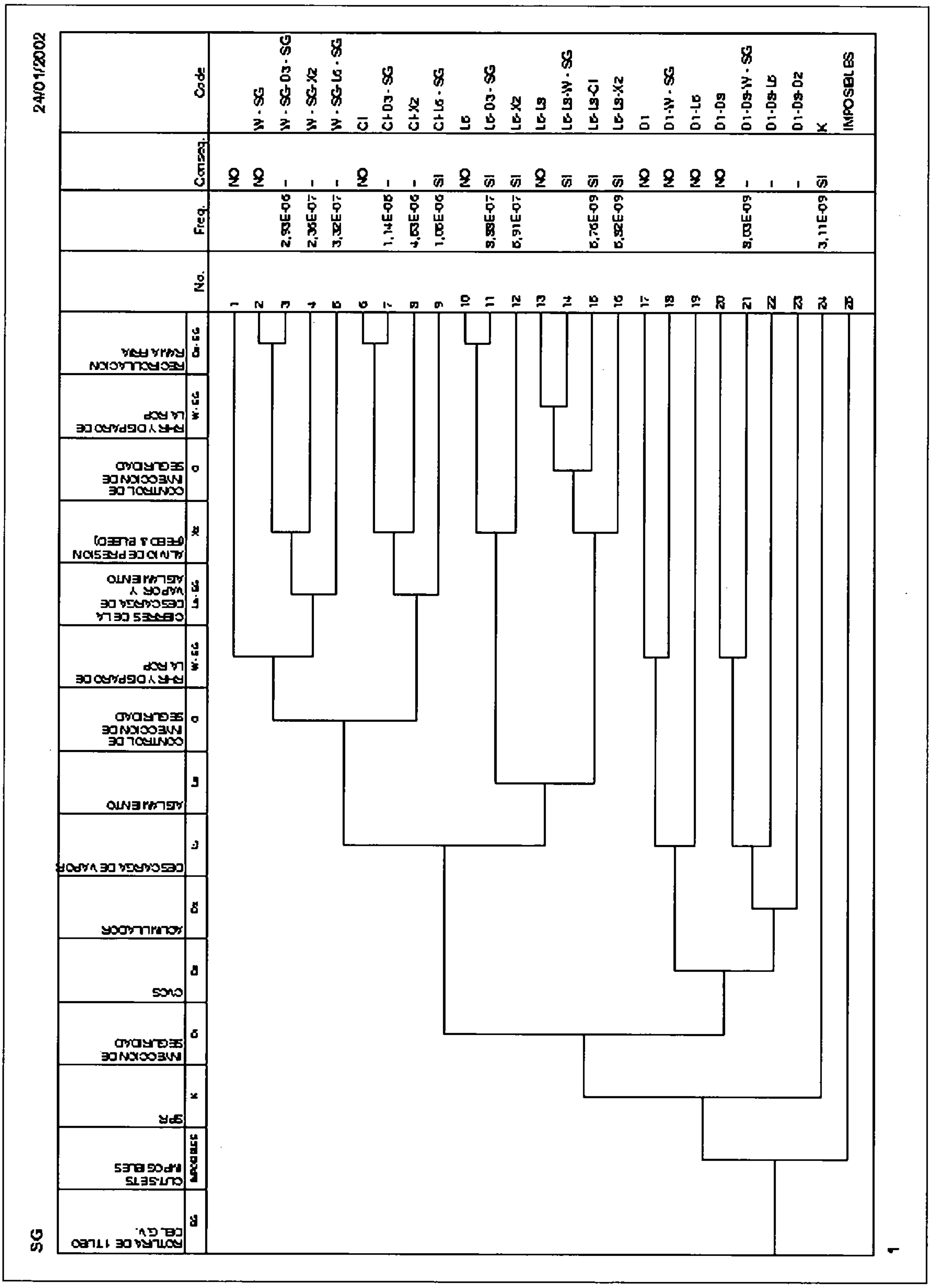

Figure 4. Event tree of the SGTR initiator showing the identified sequences.

IV. CSN capability on classical PSA studies and applications

IV. CSN capability on classical PSA studies and applications

As shown in the preceding examples, PSA event tree verification and quantification does identify potential protection problems where regulatory action is required. In order to ensure a rational dialogue with industry and to precisely understand industry positions, we have also developed a complementary approach to assimilate and acquire an independent capability to reproduce portions of the classical PSA work. This process took place from the very beginning of our work and it continues as a permanent task.

To this aim, we have taken a unified modeling and simulation point of view that removes ambiguities and allows in-house interpretation of the classical methods. First, we have defined what we understand by a well-posed PSA problem or subproblem. Second, we have precisely defined the process by which the overall problem is subdivided in simpler PSA subproblems and, finally, we have collected/adapted/developed simulation tools to resolve individual subproblems.

IV.1. PSA problem description. Reference integrated codes. Block diagrams and headers

To illustrate the approach we take PSA-2 as an example that includes most aspects of this issue. The setup of the problem is made with the help of one or more of the so-called integrated codes, able to describe all phenomena and the system impact on the dynamic evolution of damage indicators. A block diagram is used to describe the interactions between portions of the code equations that calculate the damage variable evolution. Arrows in the block diagram represent boundary condition variables to the blocks. Many feedback effects among the blocks are expected but only a handful of overall boundary conditions will be activated to trigger the simulation of the initiating event.

The essence of the diagram is the completeness of the input-output, feedback and feedforward description. These diagrams play an equivalent role to engineering P&ID diagrams and can be made more or less detailed. For a given code, the maximum detail is achieved when the number of input variables to blocks is minimum. To describe the overall PSA problem, however, a high level (low detail) block diagram may suffice. Figure 5 shows the block diagram corresponding to the MELCOR code, including as block names the associated code packages. Note that several codes may have similar high level blocks, but for a given code the blocks are basically unique, providing an unambiguous description of the structure of the dynamics of the systems and phenomena considered during a progression interval. Block diagram writing 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. This way, all the event tree header candidates may be explicitly identified. When set points or alarm conditions are activated, the sequence of events is

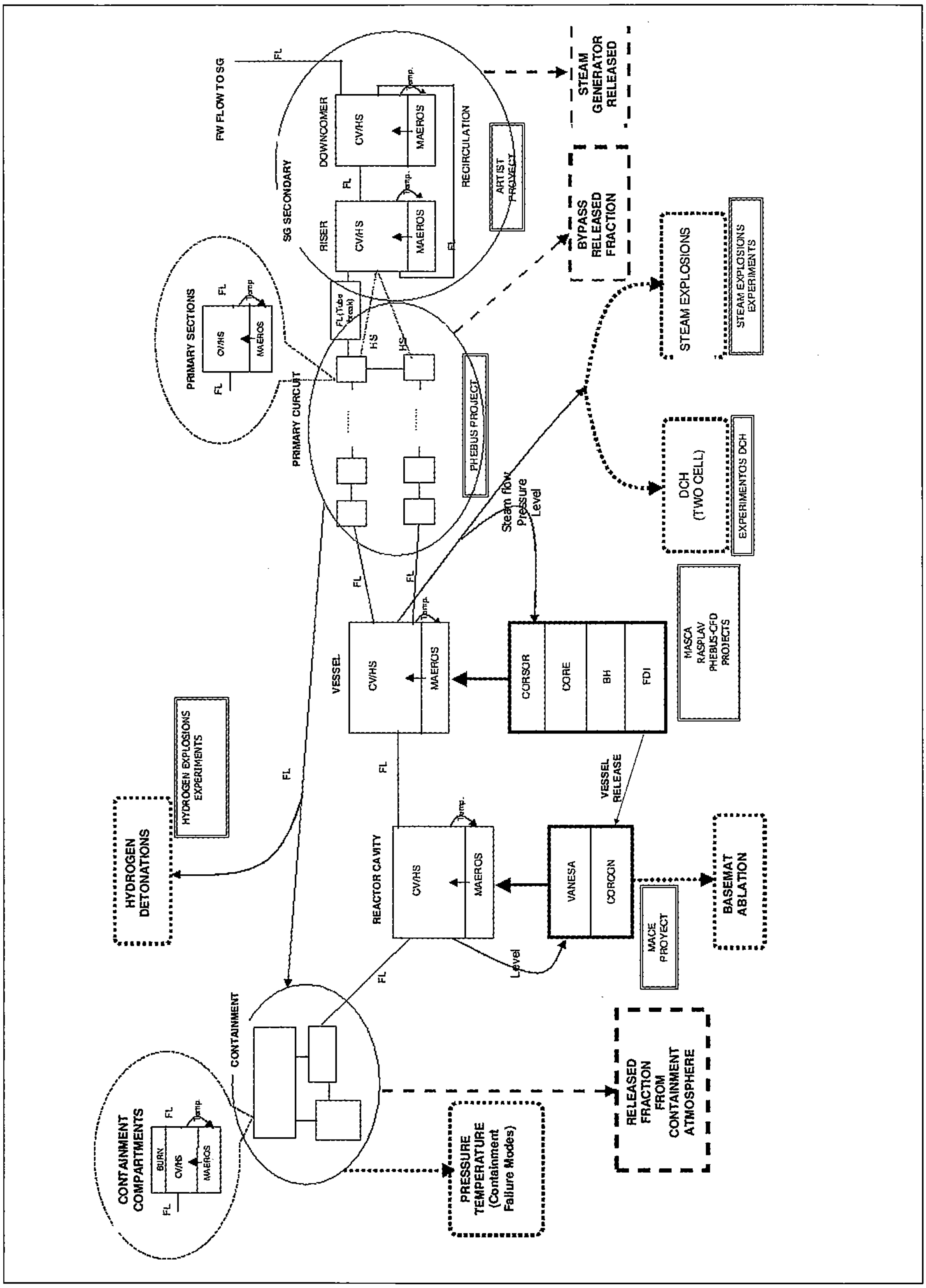

Figure 5. Block Diagram of processes for the MELCOR code

launched. However, it is difficult to ascertain without simulation the activation conditions and sequences. On the other hand, once the stimulus is 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, we consider that a PSA problem is well posed if the risk acceptance curve for this variable has also been established and the reliability Boolean models of the system and phenomena[5] headers are available. Of course this includes availability of computing codes to calculate the frequency of the Boolean sequence of failed or successful headers, as they arise through the simulation.

IV.2. Division into subproblems

Usually the problem is divided into smaller subproblems, each of them equally well posed, by using several techniques that depend on whether we are dealing with a vulnerability or accident management problem and the nature of the progression interval.

Let us exemplify the vulnerability analysis of a PSA-2. The calculation of the sequence frequency and its uncertainty band is the main focus in this case. Usual techniques are:

- Analysis by accident progression phases (in-vessel/ex-vessel, early or late), defined by the appearance of different phenomena. Each phase generates precursor sequences for the next, much like PSA-1 sequences are precursors for PSA-2.

- Subproblems associated with necessary conditions for source term damage (for instance different modes of vessel and containment ruptures).

- Subproblems associated with loosely coupled plant system sets, like containment, reactor and its cavity, the primary reactor coolant and the balance of plant systems. Boundary conditions in between these plant subsystem areas, particularly the core and reactor cavity degradation, ought to be addressed.

Each subproblem for the different phases, failure modes and plant areas is characterized by attributes that then classify and group partial event trees involving both system and phenomenon related events. Common attributes couple the subproblems and allow to synthesize an overall system event tree and overall APET. The system portion of the event tree is handled with usual boolean techniques and their cut sets grouped by system attributes (plant

[5] The actual treatment of the probability of phenomena is more complex. See reference [47]

damage states, PDS). For each damage state, the APET subsequences are then grouped again by source term attributes. Techniques are necessary to evaluate the APET probabilities conditioned to PDS and their uncertainty band. These 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. An example of the MELCOR block diagram and headers for the basemat melt-through failure mode subproblem is shown in figure 6.

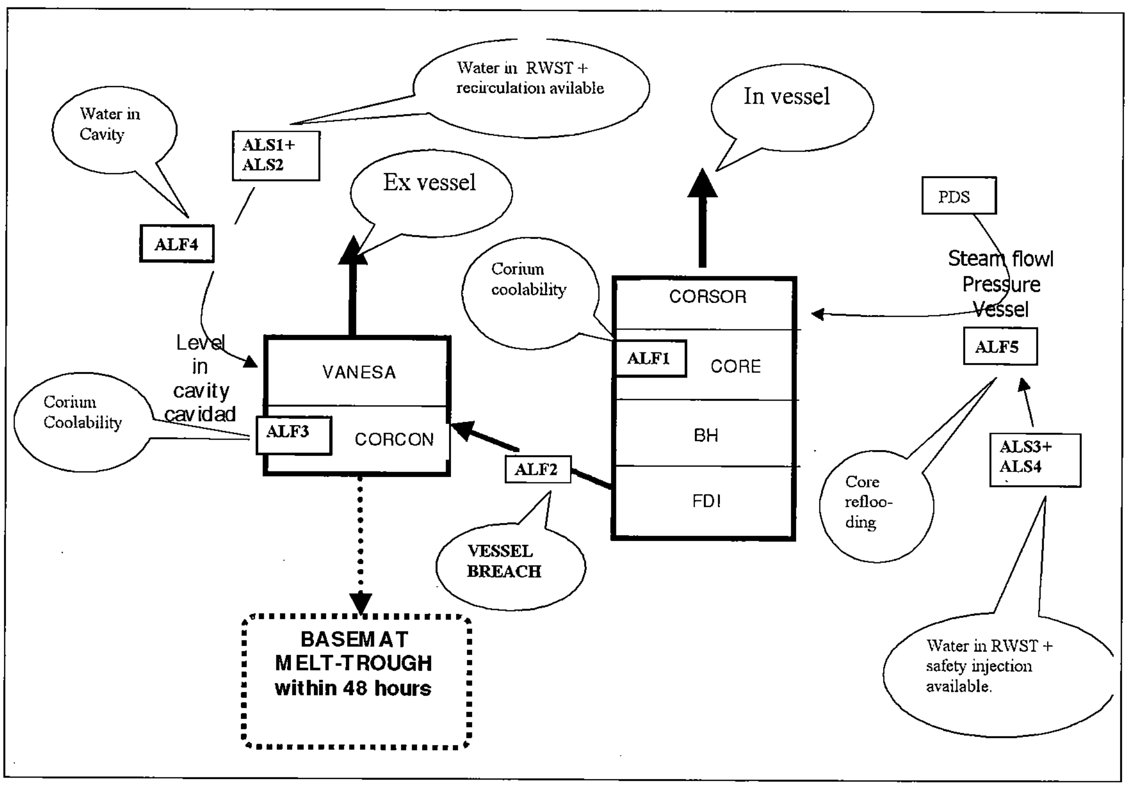

Figure 6. Block diagram and headers for basemat melt-through containment failure mode.

The partial APETs for each subproblem are synthesized into a unique APET for each plant damage state, and the probability of each branch is evaluated separately [74,75,47]. Specific computational steps are devoted to clearly represent and interpret the input and output files as for example those in figures 7 and 8 for the EVNTREE code that implements the APET quantification. Figure 7 depicts the relationships between the questions (branches and cases) for a partial APET. In Figure 8 the trajectories leading to the Very Early failure mode of the Containment are traced, showing the portion thereof that is truncated because of low (conditional) probability.

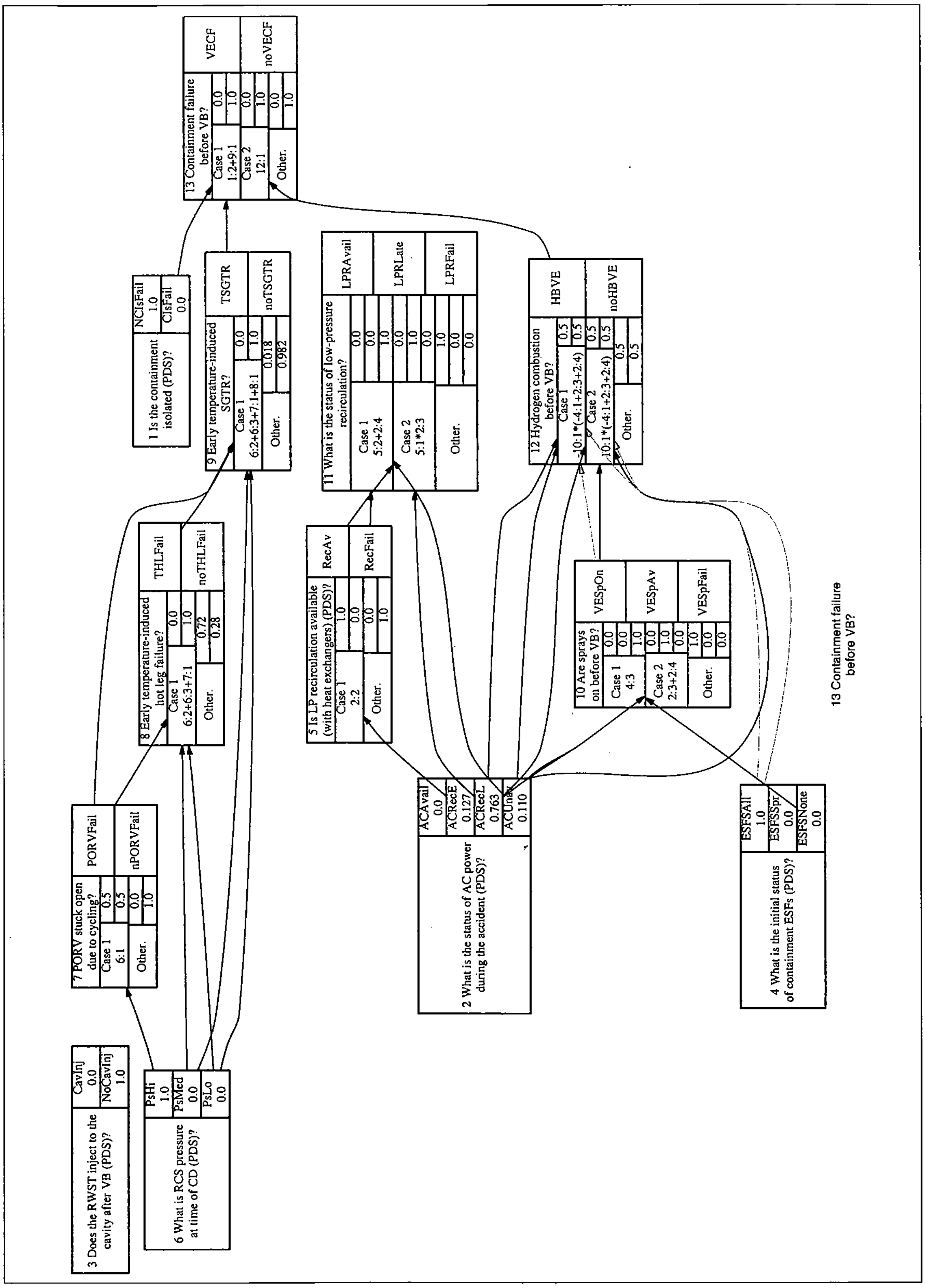

Figure 7. Input structure and internal relationships of the "Very Early" phase of a PSA-2 problem

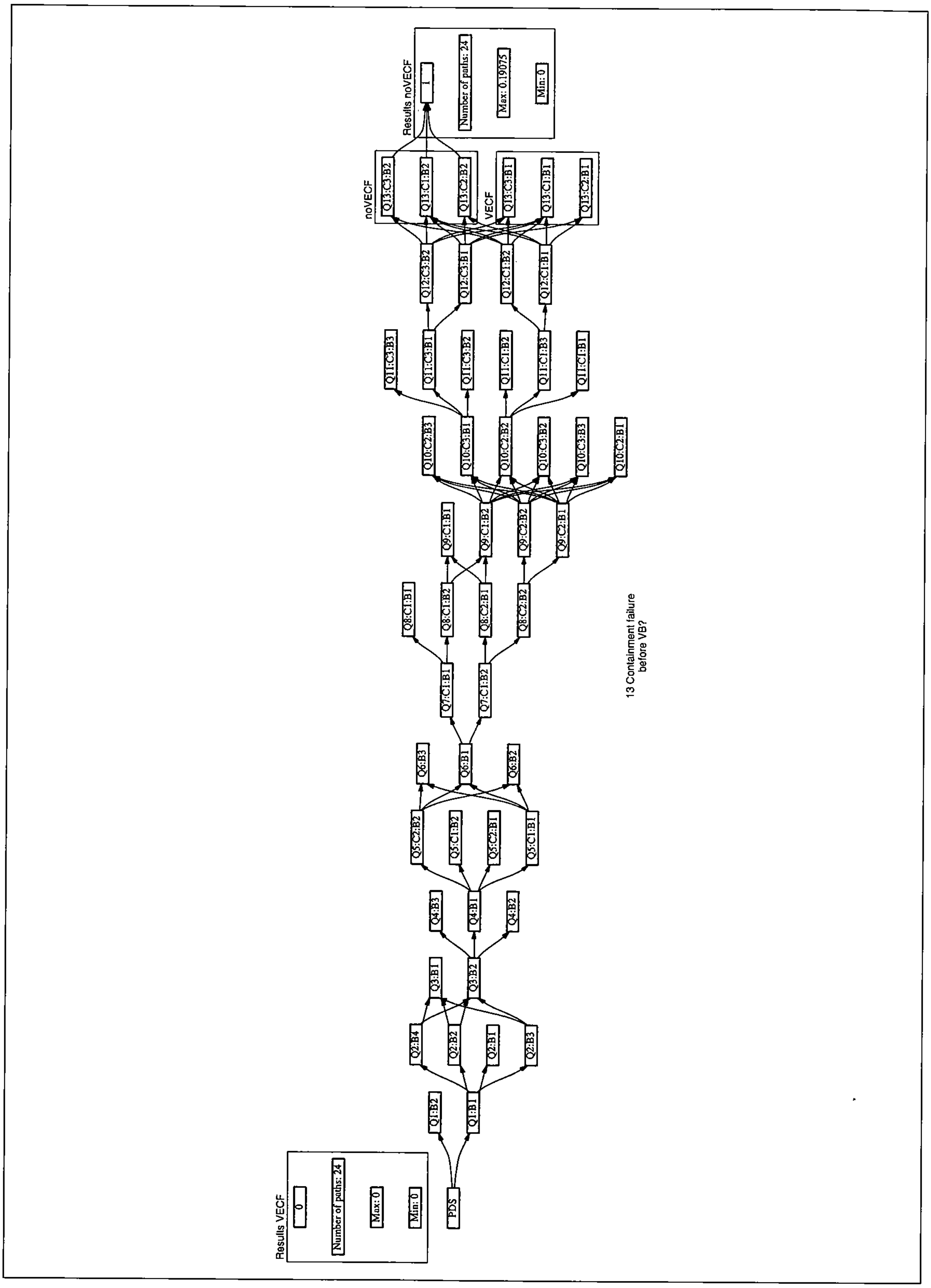

Figure 8. Output paths and final probability for the "Very Early" phase of a PSA-2 problem

IV.3. PSA applications. Boolean calculations. Probabilistic Incident Analysis (Precursor Analysis)[6]

By Probabilistic Incident Analysis we understand the revision of the results of a PSA analysis for a given incident, be it an initiator, a set of system unavailabilities, or a combination of both. The technique maps the incident into the actual plant PSA, by identifying basic events that occurred (or modifying the Boolean modeling to be able to do it). It then takes as certain all failed basic events during the actual incident and recalculates the affected sequence results. Incident analysis is routinely made at CSN, the probabilistic analysis being performed only when recommended after an incident screening process [76,77].

The exercise is substantially a Boolean requantification usually performed with the RiskSpectrum tool [78]. CSN has incorporated this type of capability as shown in the following example in one of our twin unit plants.

> "A bad line-up after a test, left a path connecting the CCW (component cooling water) systems of both units. When later on, a test was conducted on the second unit, the CCW system behaved abnormally, with several stops and start-ups of the pumps, that also entailed stop and start-up of the service water pumps, leaving the RCPs uncooled for some minutes."

The results for the conditional core damage frequency and probability can be seen in table 2. The use of new methodologies (see section V) will also improve the understanding of this PSA application [55,79,80,81].

Table 2. Conditional core damage frequency and probability results for the event

CCDF per year			
Loss of CCW (sequence)	APS rev. 3 (CDF per year)	Potential IE (CCDP)	(CCDP) Real IE
S4	$1.68 \cdot 10^{-9}$	n/a	n/a
S6	$9.34 \cdot 10^{-8}$	n/a	n/a
S8	$< 10^{-11}$	$4.09 \cdot 10^{-4}$.	$2.76 \cdot 10^{-3}$
S10	$1.57 \cdot 10^{-8}$	$1.09 \cdot 10^{-8}$	$4.21 \cdot 10^{-8}$
S11	$6.20 \cdot 10^{-10}$	$1.17 \cdot 10^{-9}$	$4.67 \cdot 10^{-9}$

[6] As indicated in section III.2 the Probabilistic Incident Analysis, usually called Precursor Analysis, is a particular case of our concept of Precursor Study.

IV.4. PSA applications. PSA-2 CSN independent results

CSN has implemented a NUREG 1150-like PSA-2 methodology [82] with the help of a consulting firm [83,84,85,86,87]. As a result, several software packages have been incorporated into the simulation system. They include tools for event tree computation (APET and separate codes for calculation of the probability of containment failure because of laminar combustion and direct containment heating), source term envelop design and exceedance curves with parametric uncertainty estimate. These packages replicate those used by CSN consultants to independently assess PSA-2 in all Spanish nuclear units. The assimilation and development of the new packages has been made in-house. Some of their results are shown in figure 9 and table 3.

Figure 9 shows the exceedance curve of the Lanthanum release fraction. Note that there is a maximum possible Lanthanum inventory and that we are in the high damage low frequency region of the risk curve. This explains the apparently different shapes of these results with the risk curve shapes shown in figure 1.

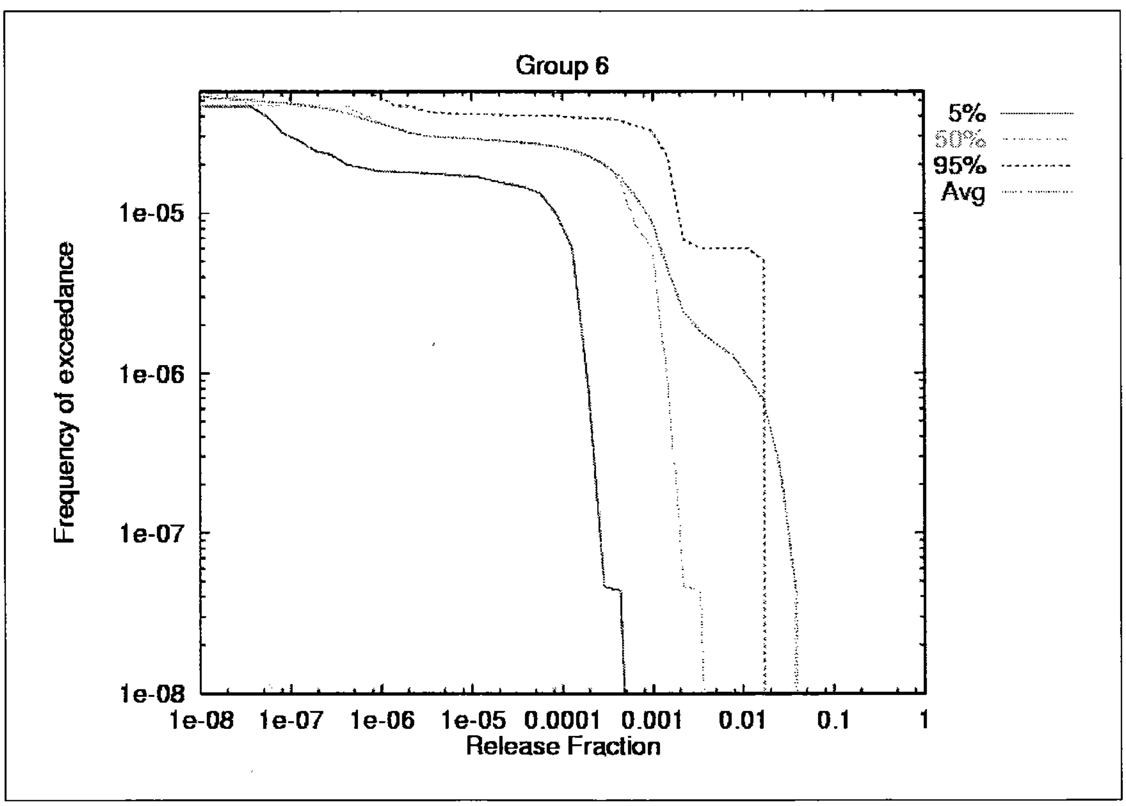

Figure 9. Lanthanum exceedance curves with uncertainty for the reference problem.

Table 3 shows frequency of different release categories (each one associated with different modes of containment failure) for each plant damage state. They are a synthesis of the PSA-2 results that allow identification of vulnerabilities by relating every number to their main cause through the analysis performed.

Table 3. Results of release categories for different PDS in the reference problem.

PDS	Frequency (per reactory year)	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12
1	1.84E-05	<0.001		0.074		0.005	0.443	0.068		0.409			
2	2.54E-06	<0.001		0.020			0.003		0.741	0.235	<0.001		
3	3.82E-07	<0.001		0.075		0.004	0.430	0.054		0.436			
4	8.55E-07		<0.001			0.070		0.929					
5	4.51E-07		<0.001	0.002	0.061	0.008	<0.001	0.150	0.107	0.670	0.002		
6	2.99E-06	<0.001	<0.001	0.063		0.015		0.194		0.727			
7	7.28E-06								0.998		0.002		
8	1.34E-05	<0.001		0.080			0.455			0.465			
9	7.92E-07	<0.001		0.026			0.003		0.676	0.295			
10	4.43E-06												1.000
11	5.69E-07												1.000
12	3.16E-06										1.000		
13	7.64E-07										1.000		
14	7.93E-07											1.000	
15	2.01E-07											1.000	
16	2.18E-08											1.000	
17	4.36E-08											1.000	
Total freq		7.49E-9	9.77E-10	2.73E-6	2.74E-8	2.03E-7	1.44E-5	2.71E-6	9.73E-6	1.72E-5	3.94E-6	1.06E-6	5.00E-6

V. Recent extensions: From static to dynamic PSA

Dynamic Reliability is today a mature approach to risk assessment in environments where the dynamic evolution of process variables is of high complexity and discrete stochastic events may continuously change the trajectories. Our developments since 1992 have been guided by these new ideas in a bottom-up approach that starts from present engineering methods and reinterprets them in the context of the general theory. In addition, it provides next step improvements by relaxing some of their restricting assumptions and then establishing a closer link between the dynamics of the sequences, the calculation of their frequencies and the human interaction through appropriate simulation environments.

Recent extensions have been oriented to:

- New developments in sequence dynamics. Generalization of the transfer function concepts for sequences of events. Its potential for PSA application as generalized dynamic release factors is under investigation [88].

- New developments in computing phenomenological probabilities for sequences of events. A new approach of Probabilistic Dynamics based on stimulus driven, random activation-time events has been recently derived. By using it, combined with cell to cell dynamic reliability techniques, a feasible, closer to present techniques, dynamic method is giving new insights [47].

- New developments about classical PSA aspects. They include rigorous definitions for concepts like available time for operations or plant damage states.

- New modeling algorithms to simulate standard PSA, correcting for dynamic effects.

VI. Conclusions
VII. References

VI. Conclusions

We have presented an overview of CSN methods and simulation packages to perform independent safety assessments to judge nuclear industry PSA related safety cases. It has been shown that this approach is excellent for an objective regulatory technical support to CSN decision making.

VII. References

[1] Izquierdo J.M., Hortal J., Meléndez E., Sánchez M., *An integrated PSA approach to independent regulatory evaluations of nuclear safety assessment of Spanish nuclear power stations,* Presented at the IBC's 7th conference on PSA in the Nuclear Industry, Café Royal, London 26-27 November, 2001.

[2] Villadóniga J.I., Izquierdo J.M., *Importance of the transient analysis in the procedure for light water reactors authorisation,* JEN-429, Junta de Energía Nuclear (in Spanish), 1979.

[3] Izquierdo J.M., Villadóniga J.I., *Basic philosophy of the nuclear regulation,* ENS/ANS Brussels Meeting.

[4] Sánchez-Perea M., Izquierdo J.M., *DYLAM-TRETA: An approach to protection systems software analysis,* in Advanced Systems Reliability Modeling, Proc. Ispra course held at ETSI Navales, Madrid, Spain, September 1988.

[5] Cacciabue P.C., Izquierdo J.M., Sanchez-Perea M., *Dynamic reliability as a tool for the assessment of protection systems software analysis,* presented at the NUCSAFE ENS/ANS Conference, Avignon, France, October 1988.

[6] Honrubia, C., Izquierdo, J.M., *Estudio genérico de seguridad de los disparos OTΔT y alto flujo neutrónico en centrales PWR Westinghouse. Influencia del taponado de tubos del generador de vapor.* Informe interno del Área de Programas de Desarrollo, 1987.

[7] García Hernández I., Fdez de Santaella A., *Proyecto de simulación de reactores BWR: Análisis paramétricos de estabilidad y análisis de comportamiento temporal,* ICAI, Junio 1989

[8] Molina D., Izquierdo J.M., Muñoz J.J., *Modelo Analítico sencillo del sistema refrigerante del reactor para el estudio de transitorios de presión de una central PWR.* VII Reunión anual de la SNE, Madrid, Diciembre 1981.

[9] Izquierdo J.M., Muñoz J.J., *Comportamiento en presión de N volúmenes monofásicos (parte 1ª),* Informe interno del Departamento de Seguridad Nuclear, Junta de Energía Nuclear, 1979.

[10] Hortal J., *Desarrollo de un modelo de válvula con actuador aplicable al análisis de transitorios de capítulo 15 de los informes finales de seguridad de CC. NN. Comparación con otros modelos utilizados,* Informe Interno del Área de Programas de Desarrollo,CSN, 1984.

[11] Gil E., Hortal J., Izquierdo J.M., *A methodology for functional testing of protection and control systems of NPP. Development of the code CAPTA.* IAEA Specialist meeting on systems and methods for aiding NPP operator during normal and abnormal conditions, 4-6 october 1986, Balatonaliga, Hungary.

[12] Mellado I., Izquierdo J.M., *Modelo para la evaluación de las pruebas de circulación natural en el arranque de CC. NN.* VII Reunión anual de la SNE, Madrid, Diciembre 1981.

[13] Izquierdo J.M., *Evaluación de las pruebas de medida del coeficiente de potencia en CC. NN. PWR*, CSN, 1984.

[14] Pérez J., Hortal J., Izquierdo J.M., Pelayo F., Sánchez M., Veci I., *Interpretación y análisis de pruebas nucleares*, XII Reunión de la SNE, Salamanca, 1986.

[15] Izquierdo J.M., Sánchez-Perea M., *Simulación de transitorios en reactor y subsistema refrigerante. Comentarios a la medida del periodo.* XII Reunión de la SNE, Salamanca, 1986.

[16] Prieto C., Izquierdo J.M., Mellado I., *Modelo termohidráulico para la simulación del comportamiento espacio-temporal de temperaturas en piscinas de combustible irradiado. Desarrollo del código PISCAL.* VII Reunión anual de la SNE, Madrid, Diciembre 1981.

[17] Izquierdo J.M., *Axial offset. Un modelo para la evaluación de seguridad de la estrategia de control de oscilaciones de Xe en CC. NN. PWR Westinghouse y de los resultados de pruebas nucleares de calibración incore-excore.* Junta de Energía Nuclear, Departamento de Seguridad Nuclear, 1979.

[18] Pelayo F., Izquierdo J.M., Hortal J., *Comportamiento y modelación de las válvulas de admisión de turbina de un PWR.* CSN, diciembre 1984.

[19] Meléndez E., Izquierdo J.M., Hortal J., Sanchez M., *Automatic generation of dynamic event trees: a tool for integrated safety assessment (ISA).* In *Reliability and Safety Assessment of Dynamic Process Systems, (eds T. Aldemir et al.)*, NATO ASI series F, vol. 120, Berlin, Springer Verlag, Berlin, 1994. *Reliability Engineering & System Safety*, 52 (1996).

[20] Devooght J., Izquierdo J.M. and Meléndez E., *Relationships between probabilistic dynamics and event trees. Reliability Engineering* & *System Safety*, 52 (1996) 197-209.

[21] Sánchez Perea, M. *Análisis y simulación de redes de subsistemas lineales mediante el desarrollo en serie de funciones de Laguerre.* Tesis Doctoral, UPC, 1996.

[22] Cojazzi G., Meléndez E., Izquierdo J.M., Sánchez-Perea M., *The reliability and safety assessment of protection systems by the use of dynamic event trees. The DYLAM-TRETA Package. Proc. XVIII Annual Meeting Spanish Nuclear Society*, Puerto de Santa María, Spain, 28-30 October 1992.

[23] Pelayo F., Pérez J., Rey J.M., Veci L., Izquierdo J.M., Hortal J., Sánchez M., *TRETA: a general simulation program with application to transients in NPPs. XIII Meeting Spanish Nuclear Society*, October 1987.

[24] Rey J.M., Izquierdo J.M., Meléndez E., Sánchez M., *Non-severe transient simulation in a PWR power plant with the TRETA system.* XVI Meeting of the Spanish Nuclear Society, October 1990

[25] Hortal J., Pelayo F., Izquierdo J.M., Sánchez-Perea M., *COLAPSO-TRETA, a compact package for stability analysis and simulation of large integrated systems application to NPPS.* International forum "Mathematical modelling and computer simulation on processes in energy systems", Sarajevo, 1989.

[26] Queral J. C., Meléndez E., Izquierdo J. M., Hortal J., Sánchez-Perea M., Herrero R., *TIZONA: A computer Code with an Advanced Two Phase Thermal Hydraulic Package,* M&C'99 conference, Madrid 1999.

[27] Sánchez Perea M., Villa J.R., Izquierdo J.M., *Linkage of TRETA computer program with SRA models. Feasibility Study.* Research contract 3220-87-08, ED Ispra, february, 1988

[28] Espinosa J.M, Garcés M., *TRETA modelling of a Spanish PWR NPP for Final Safety Analysis Report Purposes, Master Thesis of the "IV Máster en Energía Nuclear",* UAM-CIEMAT, January 1995

[29] Gª Zamorano M.A., Queral J.C., Hortal F.J., Remacha M., *Modelación de la vasija de un reactor BWR/6* , 22 Reunión de la SNE , Santander, 22-26 de octubre de 1996.

[30] Gª Zamorano M.A., Gª de la Rua C., Queral J.C., Hortal F.J., Triviño M., *Modelación de los sistemas externos a la vasija de un reactor BWR/6,* 22 Reunión de la SNE , Santander, 22-26 de octubre de 1996

[31] Devooght J., Smidts C., *Probabilistic reactor dynamics. I. The theory of continuous event trees,* Nucl. Sci. Eng. 111, 229-240, 1992a

[32] Smidts C., Devooght J., *Probabilistic reactor dynamics. II. A Monte Carlo study of a fast reactor transient,* Nucl. Sci. Eng. 111, 241-256, 1992b.

[33] Devooght J., Smidts C., Probabilistic dynamics: the mathematical and computing problems ahead, Proceedings ARW NATO ASI, Series F, Springer Verlag, Vol. 120, pp. 85-100, 1994a.

[34] Devooght J., Smidts C., *Probabilistic dynamics as a tool for dynamic PSA. Reliability Engineering & System Safety,* 52 (1996) 185-196

[35] Sánchez-Perea M., Izquierdo J.M., Queral C., Herrero R., Hortal J., Meléndez E., Muñoz R., *Role of fast Runnning 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.

[36] Hortal J., Izquierdo J.M., *Application of the integrated safety assessment methodology to the protection of electric systems. Reliability Engineering* & *System Safety*, 52 (1996) 315-326.

[37] Vanderschaft, A.J., Schumacher, J.M., *Complementarity modeling of hybrid systems.* Report BS-R9611, CWI Amsterdam.

[38] Schumacher, J.M., Geerts, A.H.W., *Impulsive-smooth behaviour in multimode systems.* Report BS-R9431, CWI Amsterdam.

[39] Hortal J., *Safety margins: deterministic and probabilistic views.* TCM J4-TC-1180. Safety margins of operating reactors and implications for decision making including considerations of uncertainties of analyses, October 15-19, 2001, Vienna.

[40] Pullum L.L., Dugan J.B., *Fault Tree Models for the Analysis of Complex Computer-Based Systems.* Proc. Annual Reliability and Maintainability Symposium, IEEE, 1996.

[41] Westinghouse Owners Group. Severe Accident Management Guidelines, 1994.

[42] Hortal J., *Simulation of operating procedures as a tool for NPP procedure verification*, Enlarged HRP meeting, Loen (Norway) 19-24th may, 1996

[43] Izquierdo J.M., Sánchez-Perea M., *Application of the integrated safety assessment methodology to the emergency procedures of a SGTR of a PWR. Reliability Engineering* & *System Safety*, 45 (1994) 159-173.

[44] Melara-SanRomán J., Sánchez-Perea M., *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.

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

[46] *Integrated Sequence analysis and New Approaches to Human Reliability (ISANEW)*, Concluding document of concerted action FI4S-CT97-0047, November 1999.

[47] Labeau P.E., Izquierdo J.M., *Stimulus-driven branchings in continuous event trees. I. Extending the theory of probabilistic dynamics. II. A cell to cell transport theory approach. III. Modelling PSA problems. Application to containment rupture probability under H2 laminar deflagration*, sent for publication to Nuclear Science and Engineering.

[48] Meléndez E., Izquierdo J.M., Sánchez M., Hortal J., Pérez-Mulas A., *Tree Simulation techniques for Integrated Safety Assessment*, Conferencia CSNI Specialist Meeting on Simulators and Plant Analysers, Espoo, Finlandia, 1999.

[49] Izquierdo J.M., Sánchez M., Hortal J., Meléndez E., *New Techniques for the Application of Dynamic Event Trees to the Interaction between Electric Grids and Generating Stations*, Conferencia conjunta ESREL'96-PSAM III, Creta, Grecia 24-28 de junio de 1996.

[50] Cojazzi G., Cacciabue P.C., Parisi P., *DYLAM-3 a dynamic methodology for reliability analysis and consequences evaluation in industrial plants, theory and how to use.* Commission of the European Communities, JRC, EURATOM, *Report EUR 15265 EN*, 1993.

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

[52] Hortal J., *Aplicación a BWR/6 del analizador de planta HIPA*, XVI Reunión anual de la SNE, Oviedo, 1990

[53] Queral C., *Algoritmo para la resolución de las ecuaciones de conservación de fluidos bifásicos. Aplicación a centrales nucleares.* Tesis Doctoral, UNED, 1995.

[54] Hortal J., Rey J.M., *Participation of Spain at HIPA*, Avignon 2-7 de octubre de 1988.

[55] Meléndez E., Muñoz R., De Gelder P., Hulsmans M., *Análisis de Precursores: Actividades del CSN en Análisis Probabilista de Incidentes*, Colección Documentos I+D 3.2001, CSN.

[56] 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.

[57] Technical Programme Committee of ICAP España, *Segundas Jornadas Técnicas ICAP-España*, ICSP-01-92, CSN, 1991.

[58] Technical Programme Committee of CAMP España, *Thermalhydraulic Analysis in Nuclear Power Plants*, Special Issue nº 13 of CSN journal "Seguridad Nuclear", IV 1999 quarterly report.

[59] Technical Programme Committee of CAMP España, *Partipación Española en el Programa CAMP. Informe de Productos y Beneficios*, Final Report of PCI CSN-UNESA AP-07 project, CSN-UNESA, 2001.

[60] Uhle J.L., Aktas B., *USNRC Code Consolidation and Development Program, 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.

[61] Prieto C., Sánchez M., *Plan de la USNRC de Consolidación de Códigos Termohidráulicos,* CSN/PIN/MOSI/0004/140, March 2000.

[62] Sánchez M., Prieto C., *Descripción de la Documentación disponible del proyecto de Consolidación de Códigos Termohidráulicos de la USNRC,* CSN/PIN/MOSI/0005/143, May 2000.

[63] Reventós F. et al., *Obtención del nuevo Código Termohidráulico Consolidado (CTC), Proc. XXVI annual meeting Spanish Nuclear Society,* October, 2000.

[64] Technical Programme Committee of CTC Spanish PCI Project, *Seminario sobre Fundamentos Teóricos del Código termohidráulico Consolidado,* Madrid, 26-28 september, 2000.

[65] Herrero R., *A standardised methodology for the linkage of computer codes. Application to RELAP5/Mod3.2,* NUREG/IA-0179.

[66] Herrero Santos R., *Developmental Results of a Computer Based Postprocessor for RELAP5/Mod3.2,* Proceedings of the Specialists Meeting of 8th Spring CAMP meeting, Madrid, May, 1996.

[67] Herrero R., Izquierdo J.M., Sanchez M., *Quality Measurement of the Simulation of Accident Evolution,* Proceedings of the TOPSAFE'98, Valencia, April, 1998.

[68] Pelayo F., Izquierdo J.M., *Aid Tools for the Interpretation of Results from TH-Codes,* Proceedings of the Specialists Meeting of 1st Spring CAMP meeting , Villingen, June, 1992.

[69] Izquierdo J.M., Sánchez M., *Non-standard termalhydraulic variables useful in the Postprocessing and Validation od CAMP code results,* Proceedings of the Specialists Meeting of 6th Spring CAMP meeting, Espoo, May, 1995.

[70] Queral, J.C., Hortal, F.J. , Gª Zamorano, M.A. , Gª de la Rua, C. Triviño, M., *Modelación de los sistemas externos a la vasija de un reactor BWR/6,* 22 Reunión de la SNE , Santander, 22-26 de octubre de 1996.

[71] Herrero R., *Desarrollo de una utilidad informática para el análisis y acoplamiento de códigos termohidráulicos empleados en seguridad nuclear.* Tesis Doctoral, UPM, en preparación.

[72] Herrero R., Izquierdo J.M., Sánchez M., *Últimos resultados obtenidos en el desarrollo del Post-Procesador Termohidráulico para RELAP5. Acoplamiento de RELAP5 con otros códigos,* Jornadas Técnicas de CAMP-España, Valencia, 27 Mayo, 1998.

[73] Hortal J., Nielsen S., *Procedure V&V by Simulation using COPMA-III. Transferring Past Experience,* Enlarged HRP meeting, Storefjell (Norway) 8-13 September 2002.

[74] Robledo F., *Asimilación de la metodología ERI. Cargas en contención en las centrales nucleares C.N. Almaraz, C.N. Ascó y C.N. Vandellós originadas por un accidente severo.* CSN/TGE/MOSI/0005/1430, CSN, 2000.

[75] Robledo F., *Asimilación de la metodología ERI. Cálculo de la probabilidad de fallo de la contención de C.N. Almaraz, C.N. Ascó y C.N. Vandellós originadas por calentamiento directo de contención.* CSN/TGE/MOSI/0103/1406, CSN, 2001.

[76] Meléndez E., Muñoz R., *CSN activities in probabilistic event analyses.* In *Proc. of the OECD/CSNI Workshop on Precursor Analysis.* Brussels, 2001.

[77] Meléndez E., *Precursor Analysis,* Curso interno del CSN, Madrid, 11-12 junio, 2001.

[78] Risk Spectrum Code Manual, RELCON, 2001.

[79] Pérez A., Meléndez E., Izquierdo J.M., *General Theory for Accident Sequence Precursors,* Proceedings of the TOPSAFE'98, Valencia, April, 1998

[80] Meléndez E., Pérez A., Izquierdo J.M., *On the application of the ISA methodology to the study of accident sequence precursors.* ESREL 97, Lisbon (Portugal) 17-20 June, 1997.

[81] Muñoz R., Meléndez E., et al., *Development of Accident Sequence Precursor Methodologies for Core Damage Probabilities in Nuclear Power Plants (NPP),* XXIV Reunión de la SNE, Octubre 1998.

[82] US NRC NUREG 1150: Severe Accident Risks. An assessment for five U.S. Nuclear Power Plants, 1989.

[83] Meléndez E., *Programas para el cálculo de la presión provocada por la combustión de Hidrógeno,* CSN, 2001.

[84] Meléndez E., *Representación gráfica de la entrada de datos y del resultado del código EVNTRE,* CSN, 2001.

[85] Hortal J., *Metodología para el APS de nivel 2: Análisis del término fuente,* CSN, 2001.

[86] Izquierdo J.M., Sánchez M., Meléndez E., *Calculation of the pressure rise due to a hydrogen combustion,* CSN, 2001.

[87] Bagüés J., Hortal J., Izquierdo J.M., Meléndez E. Robledo F., Sánchez M., *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.

[88] Labeau P.E., Izquierdo J.M., *Transfer functions and sequences of events,* in preparation.