
J. M. Izquierdo Rocha, J. Hortal Reymundo, M. Sánchez Perea, E. Meléndez Asensio
Modelling and Simulation Area (MOSI), Nuclear Safety Council (CSN) of Spain
Justo Dorado, 11
28040, Madrid, Spain
jmir@csn.es, fjhr@csn.es, msp@csn.es, ema@csn.es

ABSTRACT

This contribution reviews CSN/MOSI activities in the development and application of a computer platform to verify consistency of deterministic and probabilistic licensing safety cases. It includes a brief summary of past deterministic developments and their more recent extensions devoted to the verification of emergency guidelines. The paper main focus is, however, in old and new developments in the probabilistic side and presents the status of its implementation in the Simulation Code System for Integrated Safety Assessment (SCAIS) computer platform incorporating the Integrated Safety Assessment (ISA) methodology. The more recent developments concerning consistency between probabilistic and deterministic aspects are emphasized.

1 INTRODUCTION. CSN/MOSI QUANTITATIVE SAFETY ASSESSMENT METHOD TO VERIFY CONCLUSIONS OF PSA INFORMED INDUSTRY SAFETY ASSESSMENTS

CSN makes intensive use of Probabilistic Safety Analysis (PSA) models in key aspects of its licensing day to day life, including inspections planning and categorization of their findings, incident analysis as well as operational aspects (maintenance rule, human reliability and safety culture). On the other hand, the operation is constrained by the conclusions of the analysis of the (automatic) design basis transients and accidents, (DSA), as reported in the safety assessments (SAR), that also include day to day requirements like those included in the Operating Technical Specifications (OTS). The overall process encompasses widely different safety studies in nature, data, phenomena and systems, each being a piece interacting in several ways with many others.

Ensuring the consistency among implicit and explicit assumptions, interfaces and conclusions is a major task of the regulatory review. The set of activities may be considered as a licensing Validation and Verification (V&V) process. Most regulatory activities are qualitative in nature, but the widespread use of computerized analysis also requires sophisticated, quantitative V&V with independent checks complementing the qualitative process. This paper summarizes some of the tools (SCAIS), methods (ISA) and results that have been (and are being) developed at CSN for this purpose, with special emphasis in the most recent ones. The main focus is in PSA related developments that may be classified according to the three main stages of a typical PSA, namely:

1 Activities made in cooperation with Universidad Politécnica de Madrid (UPM) and NFQ S.L.
1. Delineate the possible sequences of events (SOE), which amounts to find all possible Sequences of dynamic Transitions (SOTs) resulting from the sequence of protective actions as well as possible failures of safety systems.

2. Any\(^2\) protective action does not take place unless necessary conditions for it are fulfilled, most often consisting of process variables entering certain regions, situations that we call stimuli activations, like alarms, procedure entry points and/or crossing deterministic setpoints. The set of transients activating stimulus is called here the stimulus domain.

3. Determine system success criteria, discriminating successful sequences of configurations of the safety systems (i.e., those where the wrong trends of damage indicators are successfully corrected) from failed ones.

4. The\(^3\) intersection of all stimuli domains of a sequence is the damage domain.

5. Compute, for each SOE, the frequency resulting from its safety systems configurations, by using, for instance, FT/ET techniques.

While detailed methods and abundant literature [1] 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 Analyses Reports (SAR) [2]. This is perhaps the most complex issue to tackle, as shown below.

2 SUMMARY OF ACTIVITIES IN THE DETERMINISTIC SIDE. NEW DEVELOPMENTS IN EMERGENCY GUIDELINES

2.1 ISA Methods Used for Sequence Delineation, Verification of Emergency Procedures, and Quality of the Set of Design Basis Transients Used in SARs (Envelope Issue)

PSA-DSA in the nuclear context is but another example of optimization of adequate protections and its verification. The main problem is to find envelops of the evolution of damage indicators in piecewise sequences of successive changes in dynamics, (i.e., SOT), associated to protection actions. In general, the problem focuses in ensuring that the envelopes consider all the possible SOT that may be involved in the accident progression and then cover, for each sequence, uncertainty in initial conditions and key data, as well as, most important, boundary conditions and protective actions 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) enveloping character.

Figure 1 deploys the strategy followed at the Spanish nuclear industry, as well as at CSN/MOSI, to ensure that all relevant situations are covered, including the division in sub-problems accounting for the accident progression (APET) ([3], [4]).

---

\(^2\) Interpretation made in the ISA methodology.

\(^3\) Same as in footnote (2).
Figure 1: Strategy to ensure that all safety relevant situations are covered.

The SAR underground philosophy is consistent with figure 1, but this approach uses the concept of “design basis transients/accidents” in order to cover all automatic action design situations. This implies the use of artificial events distorted both in assumptions and models, so that the timing of these analyses is also artificial. It is not simple to see the equivalence with the sequence delineation because of the different purpose. Any PSA invoking SARs should be aware that they provide no clue to answer important issues as the available times embedded in the success criteria. Neither they guarantee the sequence delineation, stage 1, that requires extensive PSA additional analysis, based on safety functions, taking into account that out of design situations are also considered, including operator actions.

Instead, the ISA-SCAIS verification method considers sequences as piecewise objects (one piece for each interval between consecutive transitions) consisting of well identified groups of transients covering all uncertainties explicitly, including time of actions and dynamic model boundary conditions as functions of time. The design domain is clearly distinguished from the general risk domain.

Reference [5] details tools, methods and several examples describing the ISA-SCAIS V&V approach for internal consistency of the deterministic analysis and the verification of the sequence delineation, that is, stage 1.

The method uses surrogate models to analyze them, models fed from the deterministic analysis. When considering deterministic–probabilistic consistency of stages 2 and 3, the approach ends up in the generation of a SCAIS data base of an adequate, best estimate set of representative transients and the corresponding identification of dynamic surrogate models (see section 4). These surrogate models consistently carry the deterministic connection while allowing for fast simulation of a myriad of transients, each stimulus variable having a different surrogate model that projects the influence of the rest of the system.

### 2.2 Verification of Emergency Operating Procedures (EOP) and Severe Accident Management Guides (SAMGS)

When verification of an emergency procedure (EOP) for scenarios without core melt is the issue, simulations are run with an automatic pilot version of the procedures, as realistic as possible, by using our procedure simulator SIMPROC [6] coupled to the automatic event tree SCAIS simulator [7]. Timing to take the actions is predetermined using info from best

---

4 This paper focus on the probabilistic side, because equivalent deterministic information has been published in reference [5] and presented in [17].
practices and as operator crew task action studies indicate. The objectives of the procedure should be met and success relative to any of the safety limits should be assured. If this is not the case, the procedure is questioned at specific points. Examples are given in reference [5]. They are part of the automatic sequence delineation verification of stage 1.

Concerning SAMGS, as a post Fukushima starting activity MOSI engaged in methods to get useful insights about severe accident scenarios typified by blackouts (SBO) [8]. As a preliminary exercise the SCAIS platform, using its MAAP system module, was used to analyze a sequence initiated by loss of both off-site and on-site AC power (Emergency Diesel Generators, EDG) in one of our three loops PWR-W plants. The set of actions is depicted in figure 2 below that identifies the emergency guides involved. Five damage indicators have been considered in the analysis:

- Core uncovery
- Core Exit Temperature (CET > 922 K)
- Peak cladding temperature (PCT > 1477 K)
- Fuel relocation into lower plenum
- Reactor Pressure Vessel (RPV) failure.

Figure 3 shows the damage domains for the same sequence obtained when considering the uncertain times of failure of the continuous, and of recovery of the alternate, current electric supply. A total of 900 simulations were run, each providing the information of one of the (uncertain) time combination points of the figure.

![Figure 2: Main operator actions taken into account in SBO sequences with Seal LOCA.](image)
3 SUMMARY OF DEVELOPMENTS AND APPLICATIONS IN CLASSICAL PROBABILISTIC ISSUES

3.1 Incident Analysis

CSN/MOSI has direct responsibility in executing the CSN incident analysis on a routine basis using a customized, classical FT/ET method in order to rank their severity and to classify them as precursors of more severe situations.

Precursor analyses [9] are performed in the framework of the Incident Revision Panel (IRP). The IRP is a cross-disciplinary group that discusses, reviews and classifies every incident reported by the Spanish NPPs to CSN. Within this group, precursor analyses are requested to obtain a measure of the risk impact associated with the incident and to have a probabilistic criterion as an input to the classification. An incident with a risk measure (Conditional Core Damage Probability, CCDP) larger than $10^{-6}$ is a precursor; and an incident
with a CCDP larger than $10^{-5}$ is a significant precursor, and is then classified as a significant event. Insights from precursor analyses are discussed within this group.

This precursor activity has evolved over the years in scope (also covering Significance Determination of inspection findings) and MOSI involvement as more PSA models were available. Some overall results are presented in figure 4.

### 3.2 Probabilistic Consistency Across Different Plants. Verifying Classical FT Quantifications

The cumulated MOSI experience in FT/ET quantification of Spanish plants with industry PSA models, include the use of, and knowledge about, different computational platforms, (substantially Risk Spectrum and CAFTA), and different modelling cultures at the different plants. As exemplified in the case of the precursors, inter-comparison between results in these different contexts is essential, but sometimes doubts appear about whether or not the same problem would give similar results in different environments. In view of this, MOSI, in cooperation with the CSN PSA licensing branch, initiated [10] an important harmonization activity. It is based on the use of tools (where they existed, and internal development where they did not) translating the different modelling formats into a unified XML language (Open PSA initiative). Additionally, tools were also used/developed to also translate the unified XML input files back to either computing environment. In addition, research projects were launched verifying the efficiency of the computations by comparison with alternate ET/FT approaches. Among them, Binary Decision Diagrams (BDD) constitute a popular alternative and one of the projects ([21], [22]) used them for this purpose.

---

**Figure 5**: System’s description and equations of the sequences of the case study.

**Figure 6**: Quantification results for the sequences: MCS vs. BDD approach.
Figure 6 shows a comparison [11] of some quantification results in a sample of realistic sequences. The case study corresponds to a “medium-sized” Event Tree (ET) of an industrial PSA study from a Spanish Nuclear Power Plant. Main headers of the ET are shown in Figure 5 that details the equations of the sequences of a large loss of coolant accident (LOCA) in a BWR (Boiling Water Reactor) plant.

4 CONSISTENCY OF DETERMINISTIC VERSUS PROBABILISTIC ISSUES.
SCAIS DEVELOPMENTAL PROTOTYPE

CSN-MOSI is working on a new approach to tackle the hard to handle consistency of stages 2 and 3, mainly success criteria V&V including available times. That is, to identify/verify the minimum requirements and the associated timing for PSA protective actions (either automatic or manual), as depicted in PSA headers, that are required for success.

4.1 The TFT+TSD ISA Approach

The approach is based on the use of the Transmission Functions Theory (TFT) [12] as the basis for dynamic surrogate models and the Theory of Stimulated Dynamics (TSD) [13] to compute the exceedance frequencies. Figure 7 summarizes TFT+TSD and its relation to each other. As indicated, transmission functions (FT in figure 7) provide the contribution $x_{ij}$ of a given input $ui$ (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 ($[G_1(s_1)]$, $[G_2(s_2)]$, etc. in figure 7), each modelling the dynamics associated to each of the time intervals between transitions that characterize a header. These products are intractable in general;
however the theory is able to find very fast algorithms for their computation in the time domain. FTs are an extension of linear systems to piecewise linear ones that keeps the nice features for the treatment of model topology division invoked in figure 1 within each interval.

Those process variables (flows injected, temperatures, pressures, etc.; $u_{ij}$ in figure 7) associated to the PSA header system safety functions (of any protective action, either automatic or manual) are modeled in ISA by a set of input variables to the TFT model. In a typical example, these model inputs represent boundary conditions that isolate the plant model from the outside through a safety system. Thus, the boundary condition variables may be interpreted as safety functions of that safety system. The approach may then be used to verify safety limits for each sequence, assuming the requirements of the protective function system success criteria (i.e., minimum flows, temperature and pressure ranges, starting times and so on) as constraints on the inputs.

TFT also facilitates the application of the TSD theory to the calculation of the contribution to the frequency of any SOT included in the failure domain in order to weight them with the FT/ET results of stage 3 (with a prior automatic check of the consistency of their success criteria and boolean boundary conditions). These contributions are then aggregated over the domain, finding this way the frequency of exceeding safety limits, i.e., the sequence success/failure criteria.

Among the virtues of this combined approach are that transition rates ($p_{l\rightarrow j}$ in figure 7) involved in the sequence headers may be functions of process variables, so it belongs to the set of dynamic reliability techniques. When these transition rates are simplified, as in the case of most HRA models embedded in the FT/ET, they may also be incorporated. For instance, most Spanish PSAs include first generation HRA models based on performance shaping factors and correlations depending on available times, both approximations being easily covered.
4.2 SCAIS Tools. Developmental Prototype

Figure 8 shows the structure of a first prototype [14] to implement the search for the damage/failure domains and the computation of their exceedance frequency. The prototype purpose is to optimize the approach by testing different strategies and algorithms ([18], [19]).

The prototype performance has been tested under some challenging situations, like the sub-problem illustrated in figure 9 that depicts the impact on the containment of an inflow of H₂ and steam as a result of a medium size LOCA [15]. Stimulus variables for H₂ combustion are those characterizing the onset of flammability containment gas mixtures, the phenomena taking place only if an ignition source is randomly available, with ignition pdf’s depending on electric supply conditions. Table 1 lists the available safety systems that generate sequences of transitions particularly hard to analyze because of the possibility of repetitive combustions, as may be seen in the results [16] of the failure domain of one sequence given in figure 9. In this case the TFT surrogate models for the physical phenomena were not yet available, and therefore they were replaced by an adequate model with two versions [16], a very simplified approach with dubious internal physical consistency, and an enlarged model basically equivalent to the MAAP code model. Table 1 shows some of the comparison results.

---

Figure 9: Containment pressure failure domain of sequence [1 2 3 4 4].

---

5 The axis variables are the times in seconds of the actions of the safety systems or the occurrence of phenomena.
Table 1: Sequence Exceedance Frequencies [1 2], [1 2 3], [1 2 3 4], [1 2 3 4 4].

<table>
<thead>
<tr>
<th>Damage stimulus 4</th>
<th>simplified model</th>
<th>enlarged model</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1 2]</td>
<td>0.0824</td>
<td>0.0495</td>
</tr>
<tr>
<td>[1 2 3]</td>
<td>0.0206</td>
<td>0.0111</td>
</tr>
</tbody>
</table>

5 SUMMARY AND CONCLUSIONS. FUTURE ACTIVITIES

Quantitative V&V activities at regulatory bodies are complementary of their qualitative reviews, and are essential in view of the ubiquity of computerized analysis included in the industry safety cases. Among the many issues involved, consistency checks are of primary importance. They require specific developments of independent tools and methods.

In particular these checks should be performed when they refer to the issue of probabilistic versus deterministic aspects which involve very difficult problems, as to verify success criteria and to discriminate when they should be consistently modified in PSA applications. For instance, relaxation of OTS (Operating Technical Specifications) justified on the basis of FT/ET computations should not be accepted without ensuring first that the FT/ET success criteria do not require consistent modifications.

We briefly described part of the efforts made at CSN to develop diagnostic tools and methods for this purpose, focusing in the success criteria and internal consistency of the probabilistic side.

Future activities will continue to consolidate, optimize and gain more experience in the specific approach followed, including generation of CSN standardized PSA models (like the USNRC SPAR models [20]) of Spanish plants that may be quality graded.

REFERENCES


[16] ZANCADA M., 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, Universidad Politecnica de Madrid, Noviembre 2012.


