The 14th International Topical Meeting on Nuclear Reactor Thermalhydraulics, NURETH-14
Toronto, Ontario, Canada, September 25-30, 2011

NURETH14- 250

APPLICATION OF THE INTEGRATED SAFETY ASSESSMENT METHODOLOGY TO SEQUENCES WITH LOSS OF COMPONENT COOLING WATER SYSTEM

C. Queral[1], L. Ibáñez[1], J. Hortal[2], J.M. Izquierdo[2], M. Sánchez-Perea[2] and E. Meléndez[2]
[1] Universidad Politécnica de Madrid, Madrid, Spain
[2] Consejo de Seguridad Nuclear, Madrid, Spain

Abstract

The Integrated Safety Assessment (ISA) methodology, developed by the Consejo de Seguridad Nuclear (CSN), Spanish Nuclear Regulatory Body, has been applied to a thermo-hydraulic analysis of Zion NPP for sequences with loss of the Component Cooling Water System (CCWS) in the context of the NEA application exercise SM2A (Safety Margin Application and Assessment). The ISA methodology allows among others to obtain the damage domain (the region where the PCT limit is exceeded) for each sequence of the dynamic event tree as a function of the uncertain times of operator actuations (secondary side cooling and recovery of CCWS). Sequences with available and unavailable accumulators (ACC) have been analyzed in order to distinguish all the possibilities (ACC demanded and successful, ACC demanded and failed and ACC not demanded). In this work, this damage domain and some parameters of every sequence have been obtained from the results of the simulations performed with TRACE code, these data as well as the time-density probability distributions of the considered uncertain parameters (manual actions) are used to obtain the exceedance frequency of the particular safety limit or damage limit. . The results show the feasibility of ISA methodology in order to obtain accurate enough regions of uncertain parameters (time delays or physical parameters) where the particular safety limit of interest is exceeded, as well as the frequency of exceeding this limit.

Introduction

As a part of the collaboration between Universidad Politécnica de Madrid (UPM) research group and Consejo de Seguridad Nuclear (CSN) an analysis of sequences with loss of Component Cooling Water System (CCWS) has been performed with TRACE code (NRC, 2008) in the context of the NEA application exercise SM2A (Safety Margin Application and Assessment). Integrated Safety Assessment (ISA) methodology intends to consider all the relevant uncertainties (occurrence times and physical parameters) that could impact the considered safety or damage limit. Nevertheless for the sake of demonstrating the method within the SM2A project, the analysis has focused on the treatment of uncertain times since they were expected to be dominant. Also, they need special attention because traditional uncertainty analysis methods could not be applicable. This analysis aimed at understanding the impact of the time needed to recover the CCW system, the time to begin the secondary side depressurization as well as the availability of the accumulators in this kind of sequences.

ISA methodology has been developed by the Modeling and Simulation (MOSI) branch of CSN, aiming to provide with an adequate method to perform a general uncertainty analysis, making emphasis in those sequences where some events occur at uncertain times. For a given safety limit or damage limit (in this paper, PCT is used as damage limit), the numerical result of this methodology consists of the damage exceedance frequency (DEF) for the sequences stemmed

from an initiating event. This is done along with the delineation of the dynamic event tree and the identification of the damage domain (DD) of the sequences that contribute to the total DEF. The damage domain is defined as the region of the space of uncertain parameters of interest where the limit is exceeded. Damage domains have as many dimensions as the number of uncertainties involved in each sequence. In the case being analysed, DD are up to two-dimensional as SLOCA occurrence has been treated as a deterministic event. In principle, DD dimensions are not limited (i.e., being n-dimensional in general; other examples of three-dimensional DD can be found in Izquierdo (2008). The UPM group has applied extensively this methodology in several projects, for more details see Izquierdo (2008a), Hortal (2010), Ibáñez (2010) and Queral (2010**).** ISA methodology introduces some differences with respect the classical Probabilistic Safety Analysis (PSA):

- Event tree headers in PSA are usually defined at safety function level, i.e., each header represents the successful achievement of a safety function. System success criteria are therefore needed to develop the header fault trees. In the ISA context, however, event tree headers represent hardware states (system trains working or not) or operator actions. ISA fault trees are used to calculate the probability of each system configuration, not to quantify failure probabilities.[1]

- In PSA event trees, header intervention (i.e., demand of a safety function) is decided on the basis of generic analyses. On the contrary, demand for header intervention in ISA is a simulation result. As a result the number of possible branches in a header is different in PSA and ISA. In PSA there are two branches for a header: failure or success, but ISA considers three possible branches for a header: demanded with failure, demanded with success and not demanded.

- The end state of a sequence is a discrete variable with two possible values: success or failure. In PSA event trees the end state of a particular sequence takes only one of these values. The end state of ISA sequences, however, is a random variable where each value has an associated probability. Success and failure probabilities are obtained from the sequence uncertainty analysis. PSA end states can be seen as a particular case of ISA end states where the only possible probability values are 0 or 1.

- In PSA a human action is failed if it is not performed within a pre-specified time interval (available time). An action delayed beyond the available time is treated as a non performed action. In ISA methodology, human actions are events occurring at uncertain times. A delayed action is still a performed action even if it is not able to avoid a damage condition (limit exceedance). As a consequence, a PSA success sequence, when analysed in the ISA context, may contain a non-empty damage domain resulting from excessive delays of protective actions.

A high level description of the methodology is given by the flow diagram of Figure 1 which shows the main methodology modules (blocks) and the overall interactions among modules; see also Izquierdo (2008a) for further more details):

---

[1] Due to limitations in the available information for the SM2A exercise about the PSA model, the only hardware configurations considered in this analysis are total failure and minimal configuration for PSA success. In a general case, however, there would be a separate header for each redundant train of safety systems or, alternatively, multi decision branching points with a branch for each system configuration.

• Block A. The Sequence Generation module performs the simulation of reference dynamic event trees (DET), allowing to identify the candidate sequences with non trivial DD (success or damage for all conditions) to be analyzed in detail in the Path Analysis module (Block B).

• Block B. The Path Analysis module takes each sequence of interest from block A (Sequence Generation), performing multiple simulations with different values of uncertain parameters and/or time delays (human actions or stochastic phenomena). Each such simulation, called a path, can end either in a success or damage state. Those paths ending in damage state are said to belong to the DD of the sequence.

• Block C. The probability and delay times quantification module provides the necessary information to calculate in Block D (Risk Assessment) the probabilities and the contribution to DEF of each sequence of interest.

• Block D. The Risk Assessment module calculates the DEF by integrating on the DD region, obtained from Block B (Path Analysis module), the frequency density function obtained from the probability distributions evaluated in Block C (Probability module).

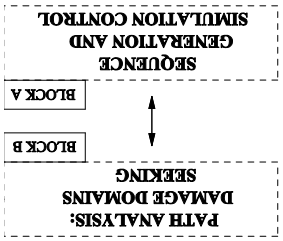

Figure 1 ISA methodology general diagram.

The analyses can be iterated to precisely define the DD border, also taking the complexity of the TH code into account to limit computing time.

1. Sequence generation module. DET simulation.

The objective of Block A of ISA is to simulate the reference DET stemming from an initiating event. At present, the simulations of DET performed by coupling MAAP (MAAP, 1994) and DENDROS are performed in an automatic way (Fernández, 2010). However, in the case of simulations with TRACE code the sequences are still simulated one by one. An automatic simulation module of DET with TRACE is being developed by Indizen in collaboration with CSN, like in the case of MAAP (Fernández, 2010).

1.1 Application to loss of CCWS sequences with SLOCA.

In a first step, several loss of CCWS event trees corresponding to PSA studies of similar nuclear power plants (Westinghouse design with 3 loops) have been analyzed to build a generic loss of

CCWS event tree in order to obtain the candidate headers for the DET analysis that is described in the next step of ISA methodology, see Figure 2. These headers could be modified depending on the results obtained from the DET simulations. From the results of this analysis it has been concluded that the following sequence headers must be considered: SLOCA (Seal LOCA); H (High Pressure Safety Injection – HPSI with 1/2 trains available); A (Accumulator Safety Injection – ACCUM, 3/4 ACC available); L (Low Pressure Safety Injection – LPSI, 1/2 trains available) which includes the recirculation phase; and S (Primary cooling, at a rate of 55 Kelvin per hour, and depressurization by means of Steam Generators - SG). Additionally, one must be aware that effective intervention of headers H and L depends on the recovery of the CCW system. That is done by adding a recovery condition (R) to the headers H and L, being now H_R and L_R. All the simulations performed in this analysis include the hypothesis of reactor coolant pumps trip coincident with the loss of CCWS event and manual control of auxiliary feedwater system.

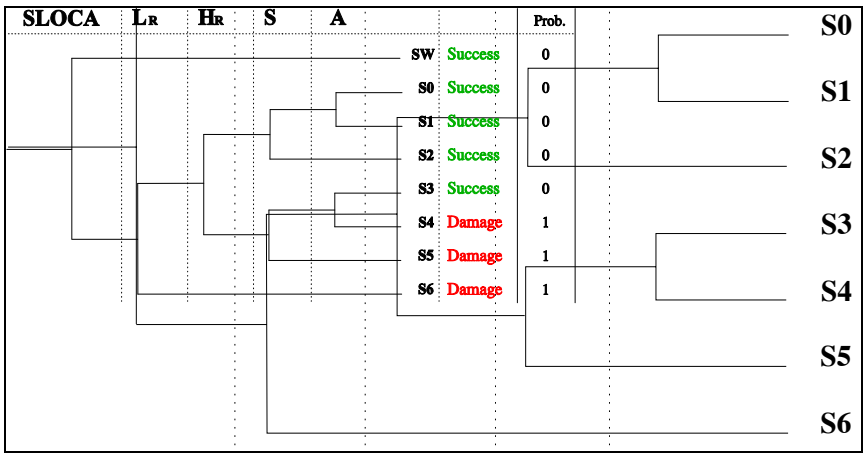

Figure 2 Generic event tree for loss of CCWS sequences

A reference DET was performed with TRACE, assuming that the CCW system is recovered right after the occurrence of the seal LOCA (which occurs at a fixed time, t=2500 s) and that all the subsequent actions represented by event tree headers occur (if not failed) without delay from the time they are required. A set of 11 sequences (sequences D) was generated. The identification of each sequence is done by the concatenation of header status: a header in upper case means success when demanded and in lower case means failed when demanded. A sample of simulation results is shown in Figure 3 and a summary of significant results for each sequence is given in Table 1. **.** Results shown in Table 1 (TRACE simulations) indicate that the headers are always demanded at the same order. However, in previous simulations performed with MAAP some headers appeared in different orders, depending on the sequence.

The information obtained from the reference DET (D sequences, without time uncertainty) allows to identify in which sequences with time/parameter uncertainty (U sequences in Figure 4) the final state is not always success or damage. Introducing time uncertainties an U sequence could be similar to different D sequences depending on the values of the action delays. For example, delaying the CCWS recovery would make sequence U0 to change from D0 to D5 due to the recovery dependence of H and L. Table 3 shows how each U sequence is related with D sequences. From this comparison, it can be concluded that for five U sequences (U0, U1, U2, U3 and U4) the end state is not always success or damage. These sequences are identified in the

generic dynamic event tree with uncertainty (GETU), see Figure 4, as sequences with "Damage Domain".

For those sequences, it is necessary to obtain their DD, i.e. the time/parameter region where the paths reach the damage condition. In these sequences the damage/success end state depends on:

- The starting time of the S header, which is a human action with a probability distribution given by the density function $h^S(t)$, t being time from the demand,
- the CCWS-recovery time, which also has a probability density function $h^R(t)$, t being time from the initiating event (which is also the demand for recovery).

Both probability distributions are described further below. The damage domains are obtained in the Path Analysis Module (Block B).

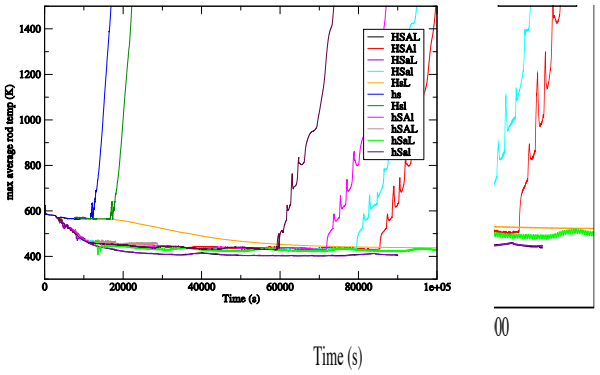

Figure **3** PCT. Reference DET of Loss of CCWS with SLOCA (TRACE code).

Table 1 Sequence information obtained from the reference DET (TRACE code)

DET Sequence	Time of H header	Time of S header	Time of A header	Time of L header	Time of PCT	PCT
D0 (HSAL)	2619	3100	5773	7400, R	0	622 K
D1 (HSAl)	2619	3100	5773	(7400, R)	99386	DAMAGE
D2 (HSaL)	2619	3100	(5773)	7400, R	0	622 K
D3 (HSal)	2619	3100	(5773)	(7400, R)	94496	DAMAGE
D4 (hSAL)	(2619)	3100	5395	11152	0	622 K
D5 (hSAl)	(2619)	3100	5395	(11152)	86748	DAMAGE
D6 (hSaL)	(2619)	3100	(5395)	10450	0	622 K
D7 (hSal)	(2619)	3100	(5395)	(10450)	61787	DAMAGE
D8 (HsL)	2619	(3100)	-	7400, R	0	622 K
D9 (Hsl)	2619	(3100)	-	(7400, R)	21934	DAMAGE
D10 (hs)	(2619)	(3100)	-	-	16631	DAMAGE

R means "demanded in recirculation phase", time value between brackets means demanded but failed

Table 2 Connection of sequences with time uncertainty and the sequences obtained in the DET

Sequence of GETU (with time uncertainty)	Reference sequences of the DET (without time uncertainty)	Final status of uncertain sequence
U0 (H_RSAL_R)	D0 D5 D8 D10	S/D/S/D ⇒ DD
U1 (H_RSaL_R)	D2 D7 D8 D10	S/D/S/D ⇒ DD
U2 (H_RsL_R)	D8 D10	S/D ⇒ DD
U3 ($hSAL_R$)	D4 D5 D10	S/D/D ⇒ DD
U4 ($hSaL_R$)	D6 D7 D10	S/D/D ⇒ DD
U5 (hs)	D10	D ⇒ D
U6 (l)	D1,D3,D5,D7,D9	D/D/D/D/D⇒ D

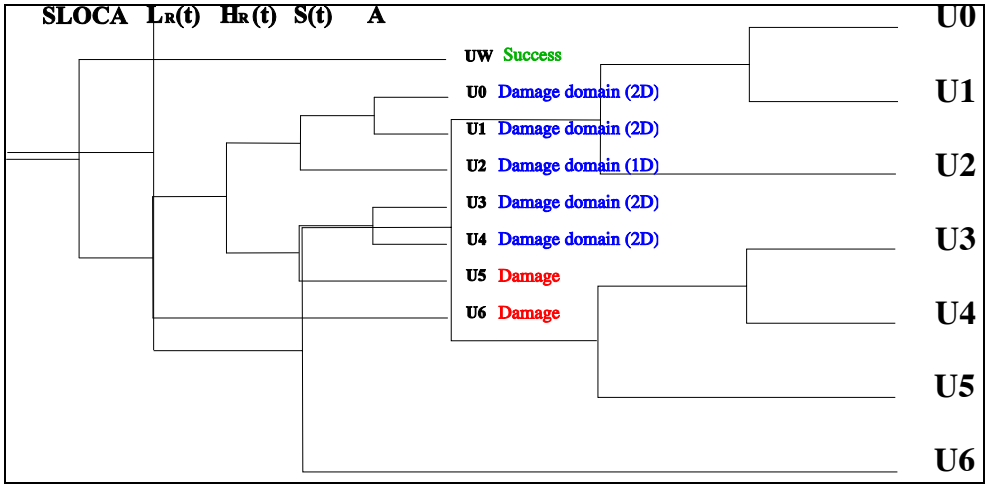

Figure **4** Simplified loss of CCWS GETU showing the sequences classified as: success, damage or damage domain.

2. Path analysis module

The Path Analysis Module (Block B) receives the sequence and parameter information of all branches of DET from the Sequence Generation Module (Block A) and determines the DD of the candidate sequences.

Headers that could occur at uncertain times (mainly operator actions but also events with stochastic phenomenology) are defined as Non Deterministic Headers (NDH). In order to take into account this uncertainty a time sampling between the minimum time when the header event becomes possible and a maximum time (or the mission time, 24 hours) is performed for each NDH, see Figure 5.

An example of how to obtain the DD of a sequence is shown in next section. If there are several non-deterministic headers and/or uncertain parameters, a multidimensional time/parameter sampling will be needed. Each sample gives rise to a path belonging to the sequence and the set of paths leading to a damage condition (i.e., limit exceedance) define the DD of the sequence.

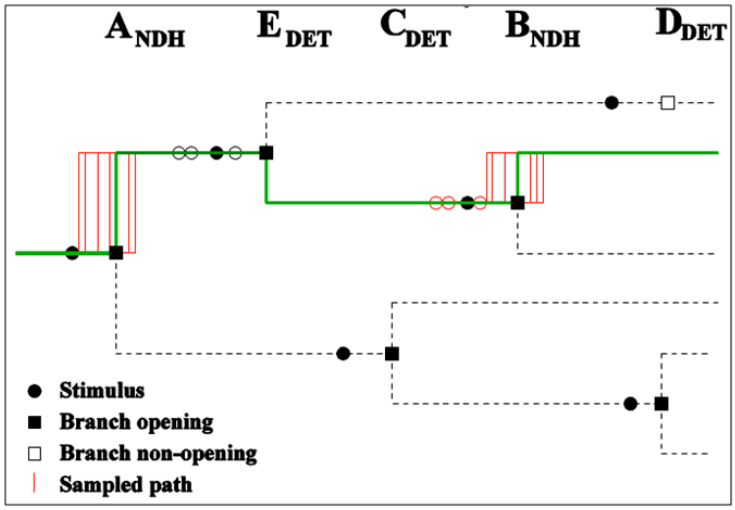

Figure **5** Path analysis in a sequence with two NDH (headers A and B).

2.1 Application to loss of CCWS with SLOCA. Simulations performed with TRACE code

In this module only the sequences with DD are analyzed. The objective of this analysis is to obtain the DD of each sequence. With the DD information it is possible to obtain the DEF of each sequence, which is carried out in the last stage of the ISA methodology (Block D: Risk Assessment) and described in the next section. As an example, the results obtained for sequence U1 (H_RSaL_R) with TRACE code are shown in detail in Figure 6. The calculation process performed in sequence U1 is the following:

1. Failure of S header is assumed, with the result of no manual depressurization in secondary side. A transient (path) is simulated for each CCWS-recovery time considered. In these sequences, damage will arrive at a certain time t0, which sets the maximum time for the (manual) start of depressurization. Starting depressurization later than t0 time is not useful to avoid damage and no more analysis is required. These time points form the line of Previous Damage (PD) above the diagonal that is shown in Figure 6.

2. Failure of recovery event R is assumed, with the result of no SIS injection due to loss of equipment cooling. A path is simulated for each time of initiation of manual depressurization in secondary side. In these sequences, damage will arrive at certain time t1, which sets the maximum time for the recovery of CCWS. Recovering of CCWS later than time t1 is not useful to avoid damage and no more analysis is required. These time points form the line of PD below the diagonal.

3. A set of paths are simulated with different times for the beginning of depressurization and CCWS-recovery times, always below the PD line. Some of the paths exceed the damage condition (red diamond) while other paths do not reach it (blue circle).

Later this analysis has been also applied to sequence U0 (H_RSAL_R). The comparison of the DD of sequences U1 and U0, see Figure 7, shows that the availability of accumulators is quite important because it avoids the core damage in a large area.

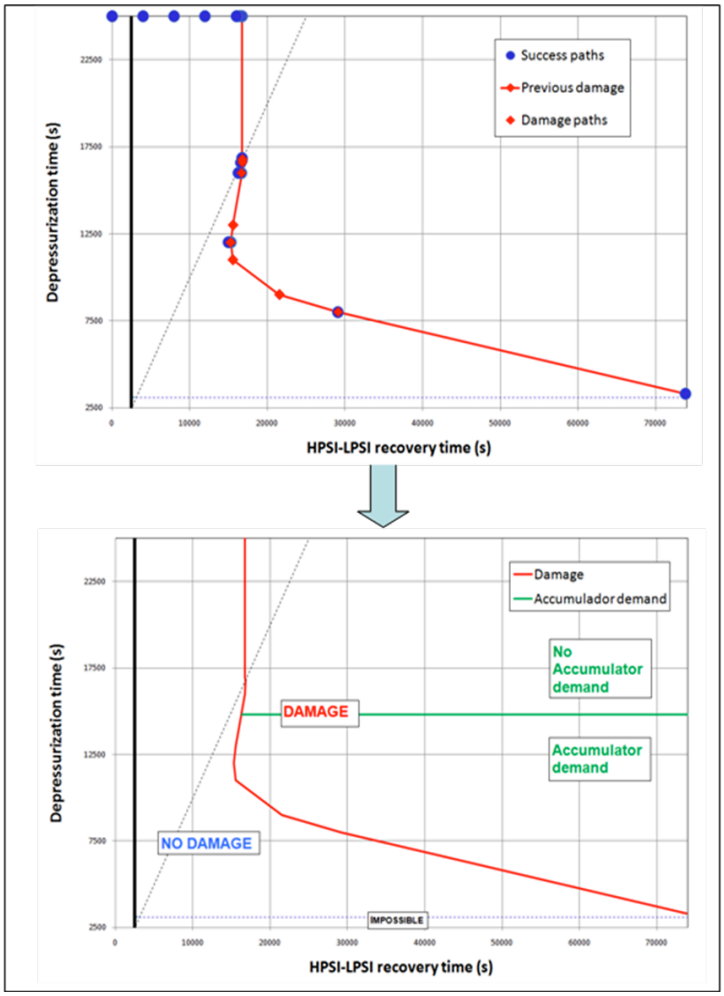

Figure 6 Path analysis of sequence H_RSaL_R. Loss of CCWS with SLOCA. TRACE code

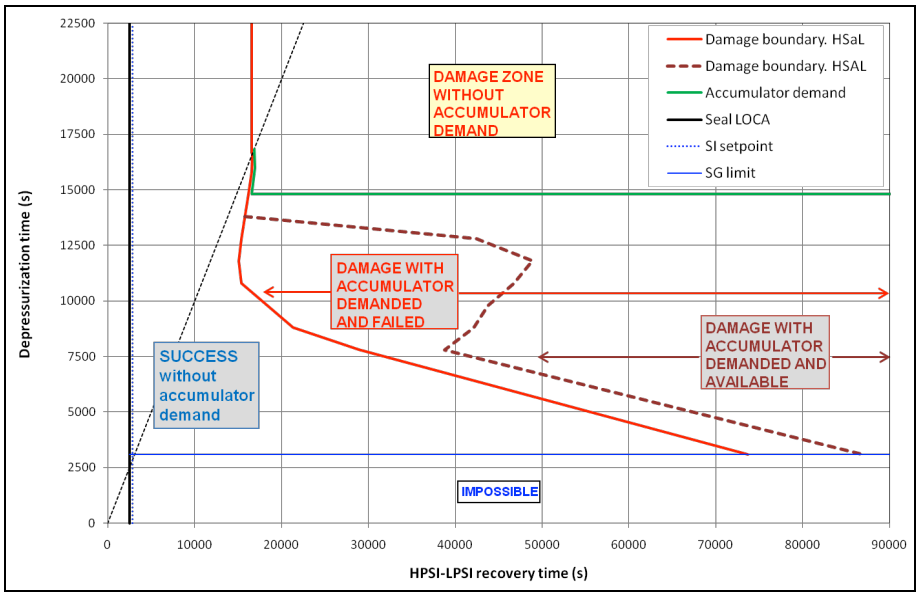

Figure 7 DD of sequences H_RSAL_R and H_RSaL_R. Loss of CCW (TRACE code)

The results of the path analysis of sequences H_RSAL_R and H_RSaL_R performed with TRACE code, shown in Figure 7, are similar to the MAAP results, shown in Figure 8, obtained in a first stage of the project (Ibáñez, 2010). The objective of the simulations performed with MAAP is to obtain a first version of the DD, this DD is refined with the TRACE code simulations. Differences in shape and smoothness on the outline of the damage domains are originated by the very different models implemented in both codes. The impact of these differences in the final results is addressed later on.

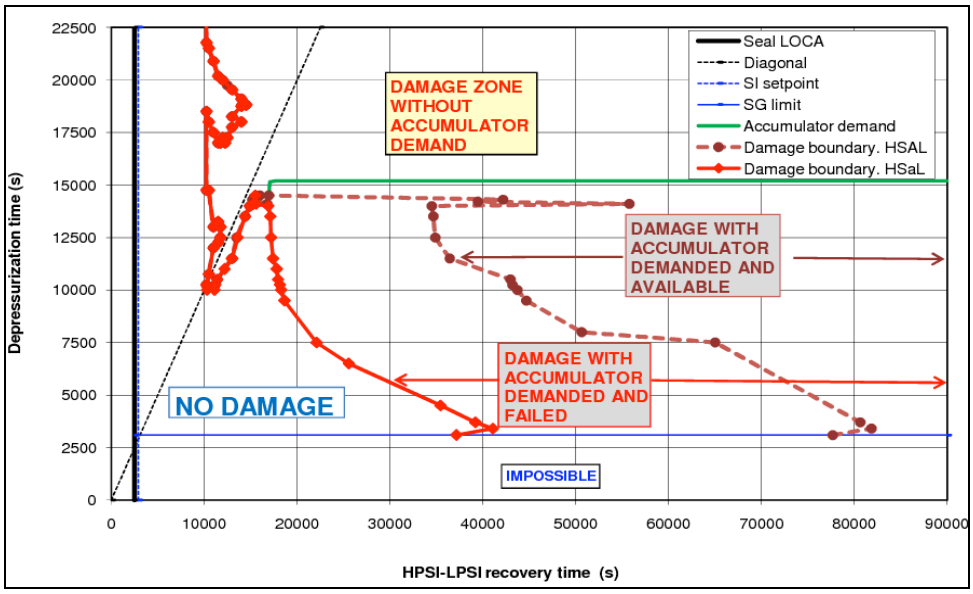

Figure 8 DD of sequences H_RSAL_R and H_RSaL_R. Loss of CCW (MAAP code)

These results also illustrate other important difference between classical PSA and ISA methods: as long as several actions with uncertain time are present in a sequence, the available time for each action becomes a function of the previous occurrence times. This effect can be efficiently afforded in ISA while only fixed, sequence specific available times are used in PSA. For example, in this analysis the available time for recovery of the CCW system is a function of the sequence (with/without ACC) but also of the starting time of depressurization action.

3. Probability calculation and risk assessment

The DEF is obtained by integrating the equations of the Theory of Stimulated Dynamics (TSD) inside the DD of each sequence (further explanation on the equations involved in this module can be found in Izquierdo (2008b)). This integration module constitutes the Risk Assessment module (Block D). The equations of the TSD evaluate the frequency density of each path of a sequence and need several probabilistic data that can be obtained from several sources like pre-existing PSA's and stochastic phenomena models (Block C). In the application of the TSD the concept of "stimulus" of a dynamic event plays a fundamental role. The stimulus of an event is a condition that makes the event possible. In the simple case of a protective action the stimulus is the demand of that action. In this analysis the TSD equations are quite simple because the stimuli of all the dynamic events are assumed deterministic, i.e., they can be directly derived from the simulation results. In addition, the probability distributions of NDH do not show mutual dependences and they do not depend on physical variables either. In other words, these

probability distributions are known functions of the delay between the activation of the stimulus and the actual occurrence of the event.

The data needed are the frequency of the initiating event (Loss of CCWS with SLOCA), the failure probabilities of the headers (H, S, A, L) and the distributions of the delays of NDH, see Table 3 and Figure 9. In SM2A exercise a more general scenario including SLOCA occurrence uncertainty was analyzed (3D-DD) and will be published in an extended paper.

Table 3 Initiator frequency and headers failure probabilities

Initiator	**Uncertainty**	**Frequency** (1/year)	**Distribution**
Loss of CCW/W		2,0E-3	
Header	**Type of header**	**Failure probability**	**PDF**
SLOCA	Deterministic	2,1E-1	---
R	Stochastic	---	Lognormal
H	Deterministic	2.2e-5	---
S	Stochastic	---	Lognormal
A	Deterministic	9,4e-4	---
L	Deterministic	5.6e-5	---

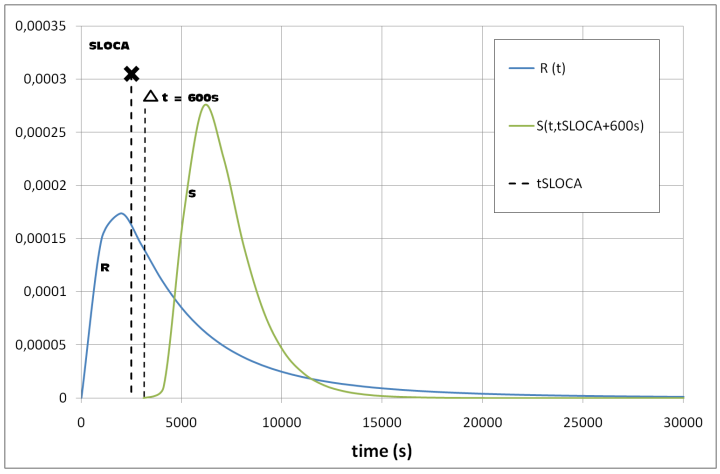

Figure 9 Probability Density Functions (PDF) of S and R.

By integrating the frequency density inside the damage domains the DEF of every sequence is obtained; the numerical integration has been performed by evaluating the frequency density in a uniform grid with integration steps $\Delta\tau_S$ and $\Delta\tau_R$ for depressurization and recovery delays, respectively. As an example the integration process for U1 sequence in the two first dimensions is shown in Figure 10. In order to show the relative importance of each region of the damage domain, the product of depressurization and recovery PDFs inside the DD is showed in Figure 11. The results obtained for every sequence of the event tree are shown in Table 4. In this table, only the sequences with blue color needed to be quantified with TSD methods. A frequency threshold of 10^{-7} y^{-1} was established for the SM2A exercise; sequences with lower frequency have not been evaluated.

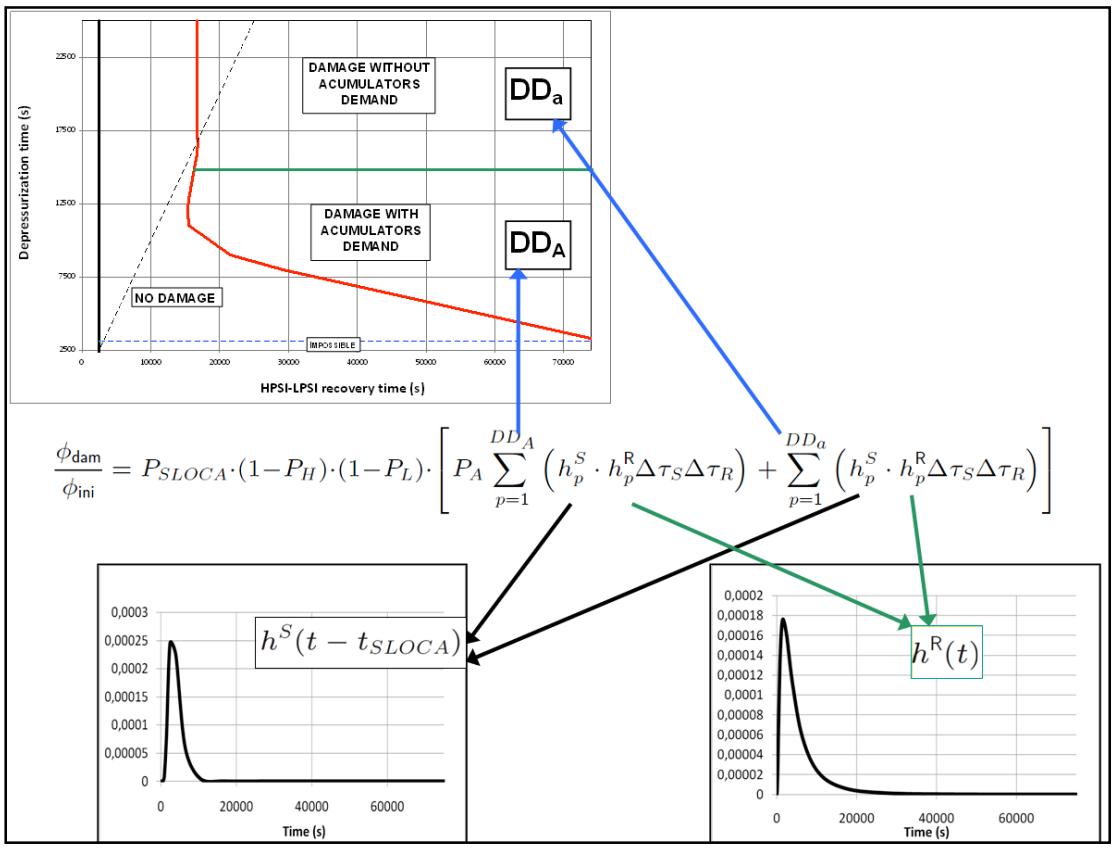

Figure 10 Example of the integration of PDF inside the DD of sequence S1: H_RSaL_R (simulations with TRACE code).

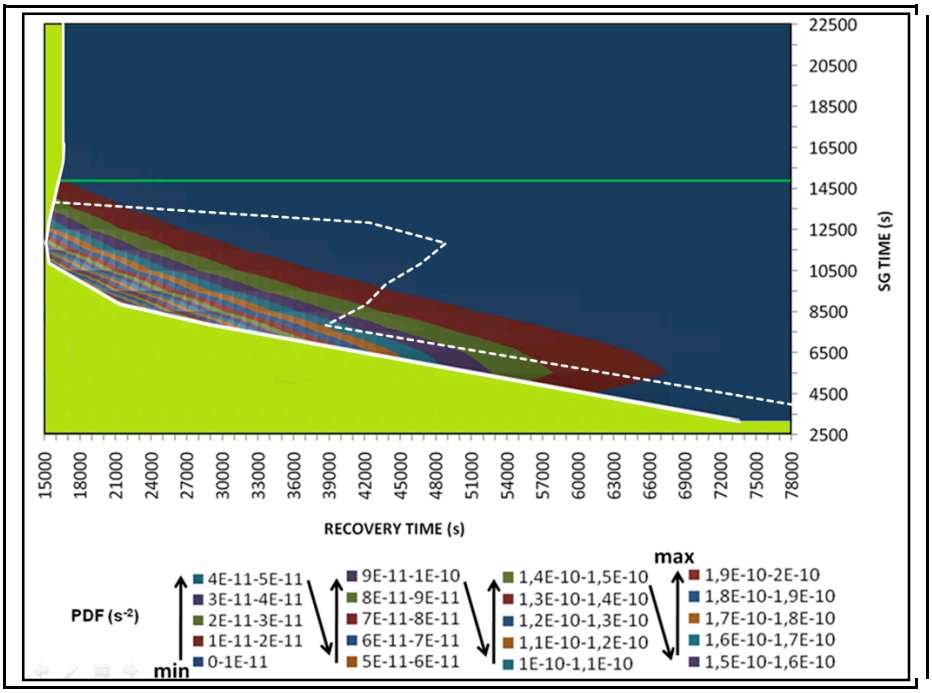

Figure 11: Probability density function inside the DD of sequences H_RSAL_R and H_RSaL_R (simulations performed with TRACE code)

Table 4 DEF of Loss of CCWS event tree (from the simulations performed with TRACE code).

Sequence of GETU	Sequence Frequency (1/year) TRACE	DEF (1/year) TRACE	Conditional exceedance probability TRACE	DEF (1/year) MAAP
UW (R and no SLOCA)	1,58E-03	0	0	
U0 (H_RSAL_R)	3,94E-04	6,69E-07	0,00170	3,80E-07
U0/U1 (H_RSL_R)	0,80E-07	0,80E-07	1	9,34E-07
U1 (H_RSaL_R)	3,71E-07	0,03E-07	0,00773	0,07E-07
U2 (H_RsL_R)	0	0	N/A	0
U3 ($hSAL_R$)	9,24E-9 < 1,0E-7	--	--	--
U4 ($hSaL_R$)	9,24E-12 < 1,0E-7	--	--	--
U5 (hs)	0	0	N/A	0
U6 (l)	0,22E-7	0,22E-7	1	0,22E-7
Total	**2,0E-3**	**7,74E-7**	**0,0004**	**13,43E-7**

It is remarkable that this result shows how the sequence frequency is distributed between success and damage so that almost any sequence can contribute to the DEF. There is also a non-null probability of sequences with non demanded accumulators; this emphasizes the need to distinguish when the lack of actuation of a safety system is due to lack of demand or to system failure. Table 4 introduces a comparison between results from MAAP and TRACE codes, suggesting that MAAP produces more conservative results than TRACE.

4. Conclusions

The ISA application performed in this paper has showed the importance of Path Analysis and Risk Assessment. In PSA each sequence has a well defined final state, success or damage. However, this analysis has pointed out that it is possible to have in the same sequence a damage probability (PD) and a success probability (PS) which fulfil that PD+PS=1.

This paper shows a practical example of application of the ISA methodology for the analysis of Loss of Component Cooling Water System with SLOCA sequences treated with two different codes, MAAP and TRACE. Although it cannot be stated as a general conclusion, comparison of both analyses suggests that the results from MAAP code tend to be more conservative than those from TRACE code.

In general, the results have shown the capability and necessity of the ISA methodology or a similar one in order to properly accounting for uncertainties in the time delay of operator response and other stochastic events along with usual parametric uncertainties in the evaluation of the safety in a NPP.

ACKNOWLEDGMENTS

This work is funded by Consejo de Seguridad Nuclear (SM2A project).

5. References

[1] Izquierdo, J.M., Cañamón, I., 2008 "Status report on dynamic reliability: Conclusions of the SDTDP/TDS methods development: Results of its application to the H2 combustion". WP5.3 benchmark Level 2 PSA. Severe Accident Research Network (SARNET). Contract FI6O-CT-2004-509065: dsr/sagr/ft 2004.074, sarnet psa2 d117 [rev1].

[2] Fernández, I. et al., 2010 "A Code for Simulation of Human Failure Events in Nuclear Power Plants: SIMPROC". Nuclear Engineering and Design (*available online 30 April 2010*)

[3] Hortal, F.J., et al, 2010 "Application of the Damage Domain approach to the calculation of exceedance frequencies" 10th International Probabilistic Safety Assessment & Management Conference (PSAM10).

[4] Ibáñez, L., et al, 2010 "Damage Domain Approach as a Strategy of Damage Exceedance Computation", Proc. Int. Conf. Nuclear Energy for New Europe 2010, Portoroz, Slovenia.

[5] Izquierdo, J.M. et al., 2008a. "SCAIS (Simulation Code System for Integrated Safety Assessment): Current status and applications". Proc. ESREL 08, Valencia, Spain.

[6] Izquierdo, J.M. et al., 2008b. "TSD, a SCAIS suitable variant of the SDTPD", Proc. ESREL 2008, Valencia, Spain.

[7] MAAP User's group, 1994. "MAAP4, Modular Accident Analysis program for LWR Power plants". Computer Code User's Manual.

[8] NRC, 2008. Division of Risk Assessment and Special Projects "TRACE V5.0 USER'S MANUAL". Office of Nuclear Regulatory Research U.S.

[9] Queral, C. et al, 2010 "Application of the Integrated Safety Assessment Methodology to MBLOCA Sequences" The 8thInternational Topical Meeting on Nuclear Thermal-Hydraulics, Operation and Safety (NUTHOS-8) Shanghai, China, October 10-14, 2010.