Proyect SMARGE
(*Safety Margins Assessment Regulatory Guide Elaboration*)

Proyect SMARGE
(*Safety Margins Assessment Regulatory Guide Elaboration*)

1 General statement of the safety problem

The safety of a facility can be defined as the limitation in magnitude and frequency of the damage that the facility can potentially generate. Damage is any undesired consequence of the operation of the facility. Damage is measured by means of variables (which we will call *damage variables*) which quantify the undesired effect. A variable measuring a damage of type p is represented by D_p. Two important characteristics of the damage are:

- It is generated as a consequence of a dynamic process.

- It is cumulative, i.e., once a given damage has been generated, it cannot be diminished.

The amount of damage generated by the facility during a given period of time depends on the nature of the undergoing dynamic processes. In normal operating conditions, it is expected that a given facility will generate damage at a limited rate, such that its cumulative effect during a given period of time (usually 1 year) is below specified regulatory limits. In addition, there could be sporadic events (here meaning disturbances of normal plant operation) resulting in impulsive damage generation. Frequent events, even if they generate small amount of damage, may significantly contribute to annual damage and its contribution must be taken into account when evaluating the annual damage generation. On the contrary, very infrequent events, even if they generate a huge amount of damage, may give a negligible contribution to average annual damage. For these cases, alternative regulatory limits must be established which limit the amount of damage to be generated by a single event.

In the case of nuclear facilities, the ultimate damage to be avoided is the radiological dose to people or to the environment, although alternative damage variables could also be considered. Legal regulations establish radiological limits to the operation of these facilities which cover both continuous operation and infrequent events. A generally known example is the US regulation which, in 10CFR20, limits the annual dose that members of the public or workers could receive as a consequence of the operation of a facility; in addition, 10CFR100 establishes dose limits for people located at given points, as a consequence of a single event.

As stated before, the level of safety of a plant is determined by its capability to limit the frequency of damage generating events and the amount of damage generated by those events. The plant safety characterization depends on the particular damage variable being considered. A plant can be considered safe only if it can be qualified as acceptable with respect to every relevant damage variable. In the following, we are considering only one damage variable, namely, radiological dose to the public at a particular location.

From the above considerations, it is clear that the concept of safety is essentially bi-dimensional. The acceptability of an "impulsive" damage of type p is a decreasing function of its expected frequency, $D_p^L(\nu)$, and can be represented by a curve in the damage-frequency plane that we may call *damage limit*. High frequency events are mainly limited because of its contribution to annual doses, which impose a very strict per-event limit, close to zero. This makes the damage limit curve asymptotically parallel to the frequency axis in the low damage. On the other side, for events of very low frequency, the acceptable damage may increase very fast as the frequency decreases and, below some frequency threshold, it cannot be technologically limited. This makes the damage limit curve to be asymptotically parallel to the damage axis in the hich damage, low frequency region.

With these considerations, the generic shape of the damage limit will be like the one represented by the curve in Figure 1.

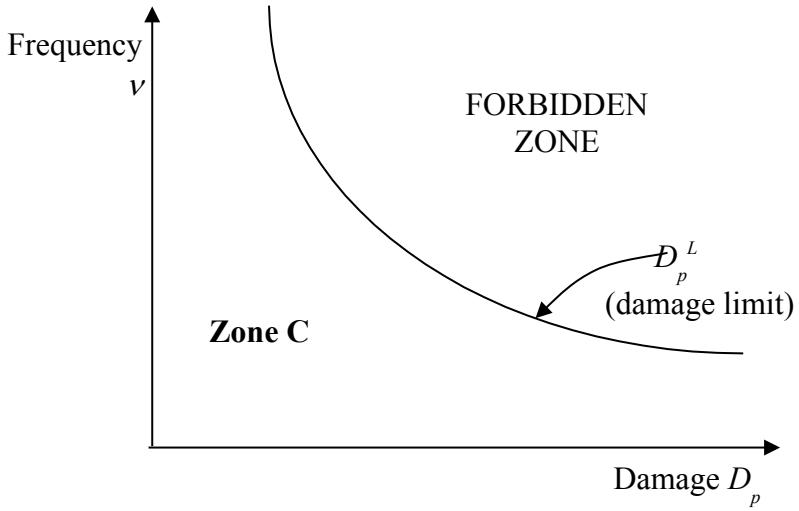


Figure 1: Generic representation of the damage limit.

In order to asses the plant safety, it is necessary to obtain some plant characteristic that could be compared against the curve in Figure 1. A given amount of damage is reached every time that an event occurs generating this damage or a larger one. The appropriate magnitude to characterize the plant safety is, therefore, the expected frequency of generation of some amount of damage or a larger one. This

magnitude is called the *exceedance frequency* of that damage. The function that relates each value of damage with its exceedance frequency is the figure of merit of the facility that can be compared with the damage limit curve in Figure 1. This is an intrinsically decreasing function that can be called the *risk curve* of the facility and it is denoted as $\nu^{ex}(D_p)$. If the risk curve totally lies in the "ALLOWED ZONE" of Figure 1 the plant can be considered safe. Otherwise, it is necessary to change the design in order to increase safety.

The estimation of the plant risk curve is not an easy task at all. Nevertheless, it is possible in many cases to demonstrate that the risk curve lies in the allowed zone, i.e., to qualify a plant as *safe*, without making an accurate estimation of the risk curve. Most methods of safety analysis aim at this goal.

Assuming that the plant risk curve can be computed, it could then be represented in the damage-frequency plane along with the damage limit. Figure 2 displays the hypothetical result of this representation. In this figure, the distance between the two curves can be properly called *safety margin*. Nevertheless, this distance is different in different regions and can be measured in several directions. An adequate definition of safety margins becomes then necessary.

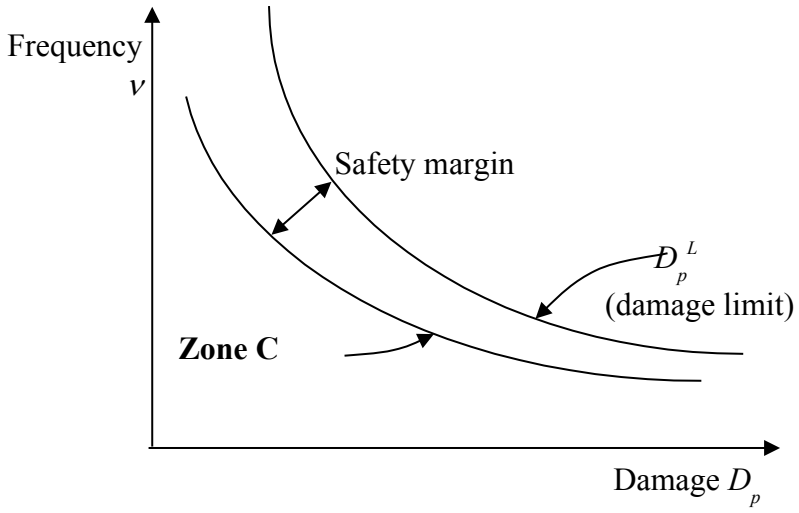


Figure 2: Representation of the risk curve and illustration of the concept of safety margin.

2 Definition of safety margins

Usually, events are classified in frequency groups. The acceptable amount of damage due to any event of a group is a function of the expected frequency of such group. The legal limits for single events are usually defined for the less frequent events considered under the design basis of the automatic protections. Lower level standards may define more strict limits for events of moderate frequency. For the latter class and for high frequency events, the potential contribution to the average annual dose generation must be taken into account and may impose more strict limits to the "per-event" damage. On the other hand, classes of events not covered by the design basis of the automatic protection should be shown to have a very low expected frequency. The acceptable frequency of these classes can be limited also as a function of the severity (i.e., potential amount of damage) of the events in such classes.

Safety margins have to be defined in terms of the risk curve. Currently, consideration of safety margins relies into the design phase, within the Design Basis Accidents analysis. As stated before, some characteristic transients are chosen and classified according to their occurrence frequency into three groups: high frequency/low damage accidents (condition II), medium frequency/medium damage accidents (condition III) and low frequency/high damage accidents (condition IV). Each condition has a maximum allowed damage limit, and if the transient analyzed surpass this limit, then it is not acceptable. Figure 3 shows schematically how this DBA analysis is made:

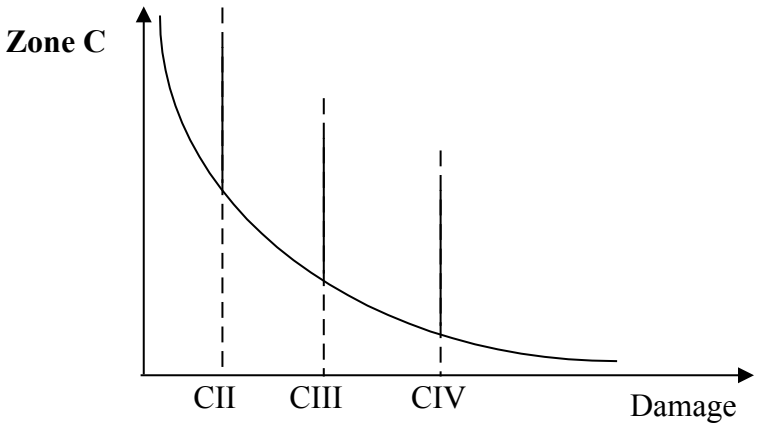


Figure 3: Current DBA analysis.

The problem in this approach relies on the selection of the transients or scenarios to be taken into account and in the selection of the DBA representative for each group of scenarios. First, scenarios should be grouped according to the damage exceedance frequency, and not to the accident occurring frequency, because if several transients happen to be properly grouped, their group frequency could eventually move them into another accident type of higher frequency (for instance, from condition III to condition II) in which the damage limit is in fact lower, and their group damage would eventually become unacceptable within the regulatory criteria. Second, there exist a lot of scenarios that might be important in terms of the damage exceedance frequency which are not considered in the Design Base (DB).

The proposal to quantitatively consider safety margins consists on establishing specific limits for the exceedance frequency to be fulfilled by each defined group of the DBA's, and to allow a fraction (exceedance frequency) of the scenarios not considered in the DB to surpass the damage limit, this fraction being different for each group. Once these exceedance frequencies have been defined, the point of the risk curve of the plant corresponding to that damage limit can be computed, and a quantitative margin can be defined as the difference between the exceedance frequency limit and the plant exceedance frequency for that level of damage. Figure 4 shows the alternative approach.

$$EFSM^{(k)} = EF_{\lim}^{(k)} - EF\left(D_{\lim}^{(k)}\right) \tag{1}$$

where

$EFSM^{(k)}$ is the Exceedance Frequency Safety Margin for the condition type k,
$EF_{\lim}^{(k)}$ is the exceedance frequency limit corresponding to the condition type k,
$D_{\lim}^{(k)}$ is the damage limit corresponding to the condition type k, and
$EF\left(D_{\lim}^{(k)}\right)$ is the exceedance frequency of the risk curve for the damage $D_{\lim}^{(k)}$.

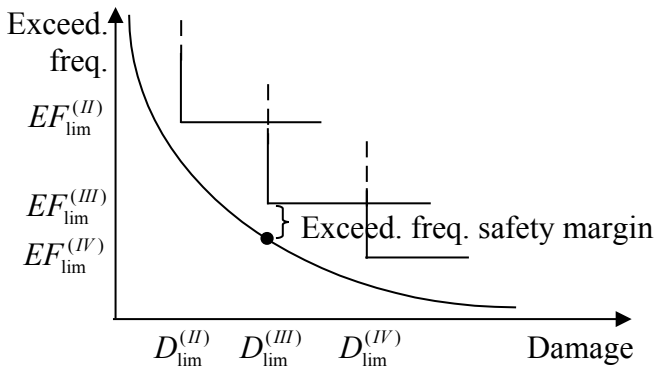


Figure 4: Proposed quantification of the safety margin

There is still one aspect of the risk curve to be considered: even if the exceedance frequency limit is fulfilled by a risk curve, it is necessary to distinguish how close is the damage of the accepted scenarios to the damage limit. Two risk curves may have the same exceedance frequency safety margin and their shape being very different above the exceedance frequency limit. Figure 5 illustrates the idea introduced here: risk curves A and B have the same exceedance frequency safety margin, but curve B has a higher damage safety margin than curve A.

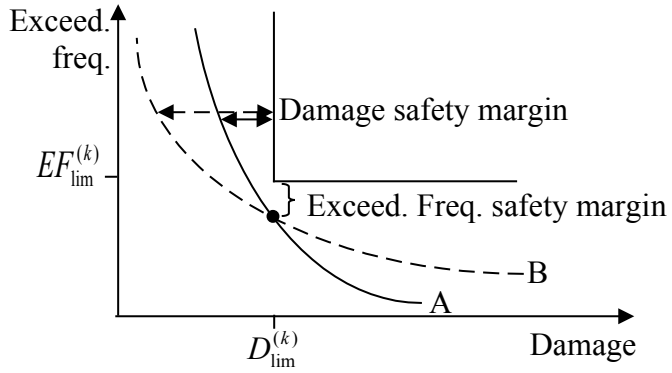


Figure 5: Considerations about damage safety margin.

There are several possibilities to quantify the damage safety margin:

- Integrating the risk curve along frequencies to get the total integrated margin between the risk curve and the damage limit above the exceedance frequency limit (see Figure 6):

$$DSM^{(k)} = \int_{f=EF_{\lim}^{(k)}}^{f=EF_{\max}} \left(D_{\lim}^{(k)} - D(EF)\right) df \tag{2}$$

where

$DSM^{(k)}$ is the Damage Safety Margin for the condition type k,

$D(EF)$ is the risk curve defined over the exceedance frequencies axis,

EF_{max} is the maximum value of the exceedance frequency considered to compute the integral, and

df is the differential element for exceedance frequencies.

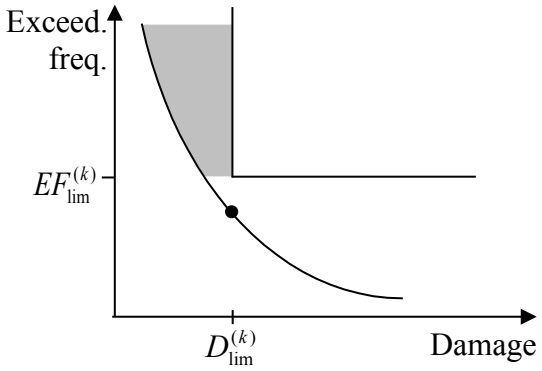


Figure 6: First possible definition of the damage safety margin.

- If we divide the previous integral by the integral of exceedance frequencies we obtain a mean value of the damage margin on that area (see Figure 7):

$$DSM^{(k)} = \frac{\int_{f=EF_{lim}^{(k)}}^{f=EF_{max}} \left(D_{lim}^{(k)} - D(EF)\right) df}{\int_{f=EF_{lim}^{(k)}}^{f=EF_{max}} df} \qquad (3)$$

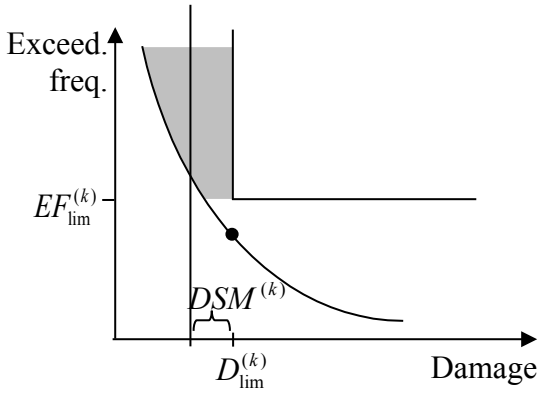


Figure 7: Second possible definition of the damage safety margin.

- Determining the frequency of transients between the damage limit point and some lower damage limit defined a priori (for instance, 90% of damage limit)(see Figure 8).

$$DSM^{(k)} = EF\left(\varphi \cdot D_{\lim}^{(k)}\right) - EF\left(D_{\lim}^{(k)}\right) \tag{4}$$

where

φ is the factor between 0 and 1 multiplying $D_{\lim}^{(k)}$ that defines the lower value of the damage interval for condition type *k*.

Let us remark that this definition of the damage safety margin is made over frequencies (not even exceedance frequencies), but reflects as well the proximity of the risk curve to the damage limit.

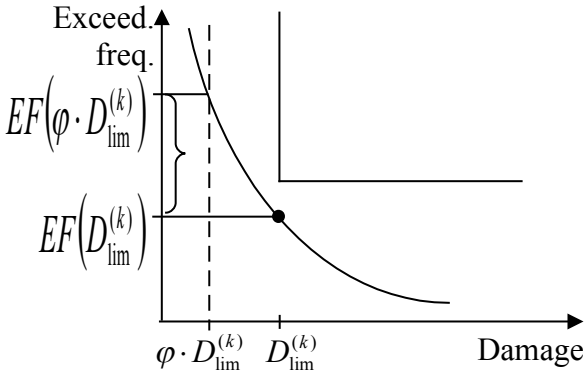


Figure 8: Third possible definition of the damage safety margin.

3 Characterization of the plant evolution: the exceedance frequency equation

Since damage generation is the result of a dynamic process, the characterization of the plant safety must be based on an adequate description of the plant states and their evolution. The plant state is described by three sets of variables. Using vector notation, each set is represented by a vector. These sets are:

- The *state vector* $\vec{x}$, a set of (generally) continuous process variables describing the dynamic behaviour of the plant.
- The *status vector* $\vec{i}$, a set of discrete variables describing the operational state of individual systems, relevant to determine the evolution of the state vector $\vec{x}$.
- The *stimuli vector* $\vec{I}$, a set of discrete variables describing the existence of conditions for a change in the plant configuration $\vec{i}$. The evolution of $\vec{I}$ strongly depends on the evolution of the state vector $\vec{x}$.

The dynamic evolution of the plant while in configuration $\vec{i}$ can be described by a set of equations of the type $\vec{x}(t) = \vec{g}_i(t - t_0, \vec{x}_0)$ with t_0 being the time when the system entered this configuration and $\vec{x}_0$ the dynamic state at that time. Since the configuration

$\vec{i}$ determines the set of dynamic equations, it can be called also *dynamics* $\vec{i}$. A change in the plant configuration, which changes the plant dynamics, is also called a *dynamic transition* or *dynamic event.*

A *stimulus* is either an order for action, issued by an automatic device or after an operator diagnosis, or the fulfilment of conditions triggering a (usually) stochastic phenomenon. It can take several different forms such as the crossing of a set-point or the entry in a region of the process variables space. In general, the term *stimulus* covers any situation which potentially causes, after some time delay, an event to occur and subsequently a branching to take place (a branching exists whenever a random event may or may not occur, and both possibilities must be considered). In addition, any stimulus may modify the probability of events directly conditioned by other stimuli. A change in the activation state $\vec{I}$ is called a *(de)activation event* (activation or deactivation); these events, by themselves, do not change the plant dynamics.

A plant transient is a dynamic process started from an initial steady state $\vec{x}_0$, $\vec{i}_0$, $\vec{I}_0$, triggered by a random instantaneous dynamic initiating event α_0 which induces a transition $\left(\vec{i}_0, \vec{I}_0\right) \rightarrow \left(\vec{i}_1, \vec{I}_1\right)$ and takes the plant away from those steady state conditions. Both the probability of the initial steady state and the frequency of the initiating event are considered known. As a consequence of the initiating event, the process vector evolves and other dynamic and/or (de)activation events will take place. The probability and the consequences of an event depend not only on the nature of the event, but also on the existing activated stimuli and on the exact times when this event and all the previous ones occurred. The consequences of a (de)activation event are changes in probabilities of other dynamic or (de)activation events, while the consequence of a dynamic event is a change in the dynamics which, indeed, may induce changes in the activation state.

Given an initial steady state and an initiating event, a particular dynamic state $\vec{x}$, it is not necessarily reachable. A reachable dynamic state, arrived at after a number n of dynamic events, can be represented by $\vec{x}_n$. The compound path resulting from the concatenation of all the plant dynamics from the initial state up to $\vec{x}_n$ may be represented by $\vec{x}_n(t) = \vec{u}_{\vec{i}_n}(t, \vec{\tau}_n, \vec{x}_0)$ where t is the time since the beginning of the transient and $\vec{\tau}_n$ is the set of dynamic transition times along the path. After the occurrence of n dynamic events, the plant configuration can be represented by $\vec{i}_n$ and the activation state by $\vec{I}_n$. An event inducing a transition from $(\vec{i}_j, \vec{I}_j)$ to $(\vec{i}_{j+1}, \vec{I}_{j+1})$ is represented by α_j.

For the purpose of safety assessment, a plant transient may be characterized by the compound probability of the set of transitions, both activation and dynamic, and by the dynamic path $\vec{x}_n(t)$ leading from the initial to the final state. Also, we may define the probability of the final dynamic state to be a synonym for the probability of the whole transient. Using the notation of conditional probabilities, and taking into account that the probability of each transition depends on the nature and the time of all the previous transitions, the (conditional) probability of a particular transient, given the initiating event and the initial conditions can be expressed as:

$$P(\vec{x}_n, \vec{i}_n, \vec{I}_n, \vec{\tau}_n \mid \alpha_0, \vec{x}_0, \vec{i}_0, \vec{I}_0) = \prod_{l=1}^{n-1} P\left(\alpha_l, \tau_l \mid (\alpha_{l-1}, \tau_{l-1}), (\alpha_{l-2}, \tau_{l-2}), ..(.\alpha_0, \tau_0)\right) \quad (5)$$

Multiplying this conditional probability by the probability of the initial conditions, $P(\vec{x}_0, \vec{i}_0, \vec{I}_0)$, and by the frequency of the initiating event, $\nu(\alpha_0)$, we obtain the frequency of this particular transient:

$$\nu(\vec{x}_n, \vec{i}_n, \vec{I}_n, \vec{\tau}_n) = P(\vec{x}_n, \vec{i}_n, \vec{I}_n, \vec{\tau}_n \mid \alpha_0, \vec{x}_0, \vec{i}_0, \vec{I}_0) P(\vec{x}_0, \vec{i}_0, \vec{I}_0) \nu(\alpha_0) \quad (6)$$

According to (1), the amount of damage generated by this transient will be given by:

$$D_p(t_{end}, \vec{x}_n) = \int_0^{t_{end}} DG_p(\vec{x}_n(t))dt \quad (7)$$

where t_{end} is the time when the final state is reached.

The frequency of exceedance of a particular amount of damage D_p (i.e., the risk curve) will result from the aggregation of the frequencies of all the transients producing a damage higher than or equal to D_p. This aggregation will take the form of an integral when summing-up over continuous variables and the form of a summation when involving discrete variables. Although the initial dynamic state $\vec{x}_0$ is theoretically continuous, only a few numerable initial conditions have a non-negligible probability. Because of that, the frequency aggregation of transients starting from different initial conditions has been expressed as a summation, not an integral. With these considerations, the expression of the risk curve will be:

$$\nu^{ex}(D_p) = \sum_{\vec{x}_0} \sum_{\alpha_0} \sum_{(\vec{i}_n, \vec{I}_n)} \int d\vec{\tau}_n \nu(\vec{x}_n, \vec{i}_n, \vec{I}_n, \vec{\tau}_n) \theta\left[D_p(t_{end}, \vec{x}_n) - D_p\right] \quad (8)$$

The integral on the vector variable $\vec{\tau}_n$ actually indicates a set of chained integrals, each one extended to the possible values of each τ_j, with the condition of maintaining the nature and the order of the transitions. The summation over $(\vec{i}_n, \vec{I}_n)$ takes into account all the possible combination of transitions, including changes in its order, starting from given initial conditions and initiating event. The summation over α_0 accounts for every possible initiating event from given initial conditions and, finally, the summation over $\vec{x}_0$ collects all possible initial conditions. In expression (8), θ is the step function which selects for frequency aggregation only those transients generating a damage higher than D_p.

The importance of expressions (6), (7) and (8) is that they allow us to identify which particular approximation of the risk curve is used in current safety analysis methods like PSA or Transient Analysis and, consequently, they uncover the relationship between these analysis methods. These expressions are the result of the Stimulus-Driven Theory of Probabilistic Dynamics (SDTPD) (Labeau & Izquierdo 2005a and 2005b), in its 'paths and sequences' approach. The SDTPD is a natural extension of the Theory of Probabilistic Dynamics (TPD) to stimuli dependency. Some further details on the SDTPD are given in the following chapters.

4 From classical PSA to SDTPD: a brief history

4.1 The PSA technique

Classical PSA techniques for the exceedance frequency computation make use of the Event Trees and the Fault Trees as probabilistic tools. The first ones account for the accident evolution by assuming a fixed sequence of protection devices interventions (headers), ordered following several sequence delineation rules given by expert judgement. The second ones compute the success/failure probability for each individual header, through the deterministic technique of the Design Basis Analysis.

The standard procedure to model the state (success/failure) of a header (top event) in the PSA environment is to build the fault tree for its safety function. The reliability modelling thus achieved has to account for all failure modes of each system with enough detail, but maintaining an adequate size. The resulting structure can be reduced by means of the boolean algebra rules to obtain a canonical form of the boolean function that represents the system failure. This canonical form is usually the Disjunctive Normal Form (DNF), also called Minimal Cut Set representation of the boolean function. There are other canonical representations of the boolean functions, Decision Diagrams being the more useful.

In an Event Tree, a sequence is identified by the status of the intervening headers. The probability of a sequence is computed multiplying (boolean) the headers that are in a failed state, also providing some way of accounting for the headers in a working state. This operation yields the boolean equation of each sequence. Summing up (boolean) all sequences, one obtains the boolean equation for the event tree. The (boolean) addition of the boolean functions gives the final core damage equation. Note however that while performing the former two operations, the product of the headers for each sequence and the addition of the sequences to obtain the final representation of each event tree can lead to reductions because of absorptions in the boolean operations, i.e., something may not happen if different initiators are combined.

4.2 Markov and semimarkov models (TPD)

Markov models are state based models where the system state j is described in terms of a collection of the state of single elements, transition among states being due to a sequence of single element failures/repairs. There is a known transition rate $p_{j\to k}$ among states j and k which is found from the addition of individual single element failure/repair rates, each one now dependent on the state of the other elements, so the order in which the single events take place to transit among two states differing in several element states do matter. It is assumed that the time evolution of the states is a Markov stochastic process, i.e. the probability π for the system to stay in a given state during a given sojourn time τ is independent on the time at which the state is entered, so state probabilities are independent on the past history (memory-less stochastic systems).

The main equation of the Markov model computes the probability π of being at a state j at time t, given by the balance equation:

$$\frac{d}{dt}\pi_j(t) = -\pi_j(t)\cdot\sum_{k\neq j} p_{j\to k} + \sum_{k\neq j} p_{k\to j}\cdot\pi_k(t) \tag{9}$$

where

j,k are binary state vectors indicating the (un)failed state of the systems, and $p_{j\to k}$ is the transition rate from state j to state k.

When transition rates only depend on the individual elements that change with the transition, but are independent on the rest of the elements, Markov models should provide the same result as the classical PSA approach. However, it is of interest an approach that is able to link the frequency of exceedance of a failure mode of a barrier with those of prior barrier failure modes, and/or with the frequency of reaching conditions required for each of them.

We summarize the assumptions made in the Markov approach:

- Events may occur at any time with a given rate, and such that the frequency of entering a given state is independent on the time of entry. This assumption is reasonable in the long term time scale for random events, as for instance during the pre-accident period, but it is not so for the sequence of consequential events following an initiator.
- On the other hand, the probability of the demand is taken to be 1 or zero, as well as the fraction of paths leading to violation of safety limits (damage). These two assumptions are further explained below.

Markov extensions for cases where the transition rates depend on process variables $\vec{x}$ are called semi-Markov models (Theory of Probabilistic Dynamics, TPD). Within the TPD, probability π of being at a combined state (x, j) at time t is given by the balance equation:

$$\frac{\partial}{\partial t}\pi_j(\bar{x},t) + div\left(\frac{d\bar{x}}{dt}\pi_j(\bar{x},t)\right) = -\pi_j(\bar{x},t)\cdot\sum_{k\neq j} p_{j\to k}(\bar{x}) + \sum_{k\neq j} p_{k\to j}(\bar{x})\cdot\pi_k(\bar{x},t) \tag{10}$$

We define the ingoing density $\varphi_j(\bar{x},t)$ as:

$$\varphi_j(\bar{x},t) \equiv \sum_{k\neq j} p_{k\to j}(\bar{x})\cdot\pi_k(\bar{x},t) \tag{11}$$

The differential equations of the ingoing density $\varphi_j(\bar{x},i,t)$ can be restated in integral form:

$$\varphi(\bar{x},i,t) = \sum_{j\neq i}\int_0^t d\tau \int d\bar{u}\,\delta\left(\bar{x} - \bar{g}_j(t-\tau,\bar{u})\right)\left[\pi(\bar{u},j,\tau)\delta(\tau) + \varphi(\bar{u},j,\tau)\right] q_{ji}(t-\tau,\bar{u}) \tag{12}$$

where

$$q_{ji}(t-\tau,\bar{u}) = p_{j\to i}\left(\bar{g}_j(t-\tau,\bar{u})\right) e^{-\int_o^t \sum_{k\neq j} p_{j\to k}\left(\bar{g}_j(s-\tau,\bar{u})\right) ds} \tag{13}$$

Within this extension, for sequences of events occurring instantaneously after crossing setpoints, and whose stimuli vector deactivate immediately after each event, the problem can indeed be reduced to a classical event tree with probability of the demand one or zero, so the classical approach remains valid.

4.3 The SDTPD technique: scope

There are frequent cases where there is a time delay since the activation of setpoints and/or when they do not deactivate after the events, (as for instance operators delays in taking potentially different actions after alarms that may remain concurrently activated). In such cases, competing event mechanisms complicate the situation. More generally, the same happens whenever for the events to occur, some conditions ought to be fulfilled that depend on the accident paths followed, conditions that may persist after the events. A typical example is the occurrence of combustion phenomena only if flammability conditions are met, delays being potentially the result of stochastic ignition conditions and with potential for multiple combustions if the flammability conditions persist. Those more general conditions, (including setpoints as examples) may be considered as stimuli for the events and when accident paths reach them we speak of the paths "activating stimuli".

Because stimuli activation conditions the events, the history of activations during the accident paths do matter in calculating the frequencies, and extensions of the Markov process equations accounting for these features are necessary. Those extensions constitute the so called Stimulus-Driven Theory of Probabilistic Dynamics (SDTPD).

5 Stimulus-Driven Theory of Probabilistic Dynamics

5.1 Mathematical description of the SDTPD

The extension of the semi-Markovian frame into a non-Markovian one yields to the stimuli-dependent SDTPD. A non-Markovian frame states that stimuli may remain activated after each event. Mathematical formulation of the probability of being in a combined state $(\vec{i},\vec{I})$ becomes fairly complicated, as many new dependencies appear explicitly that did not exist in the previous formulations. To simplify notation, from now on the combined state vectors $\vec{i}$ and $\vec{I}$ will be denoted as *i* and *I* respectively.

As the scope of this report is not to present a detailed mathematical derivation of the SDTPD equations, we invite the interested reader to check the references ????. Here we will just present some discussions on specific details of that formulation.

In (Labeau & Izquierdo 2005a) (in the sequel 'paper 1'), the non-Markovian approach assumes that, for dynamic transitions, from all the stimuli that are activated before the transition (set *A*'), only some of them remain activated after that transition (subset $A \subset A$'). However, the change of state of other stimuli within (de)activation events is not considered. With this remark in mind, the integral equation for the ingoing density due to a dynamic event is:

$$\varphi_{in}(\bar{x},i,t,\bar{\tau}_A,A)=\sum_{A'\supset AF\in A'}\sum_{j\neq i}\int d\bar{u}\int_0^t d\tau^*\int_0^{\tau^*}d\tau\int_0^{\tau^*}\ldots\int_0^{\tau^*}d\bar{\tau}_{A'/A}\,\delta\left(\bar{x}-\bar{g}_j(t-\tau,\bar{u})\right)p_{ji}^F\left(t;\tau^*,\tau,\bar{u},\bar{\tau}_{A'},A'\right)$$
$$\times\left[\varphi_{in}(\bar{u},j,\tau^*,\bar{\tau}_{A'},A')\delta(\tau^*-\tau)+\sum_{G\in A'}\varphi_G(\bar{u},j,\tau^*,\tau,\bar{\tau}_{A'},A')\delta(\tau^*-\tau_G)\right]\delta_{ji}^F(A'\to A)$$

(14)

with

$$p_{ji}^{F}\left(t;\tau^{*},\tau,\bar{u},\bar{\tau}_{A'},A'\right)=\frac{\tilde{h}_{ji}^{F}\left(t-\tau;\bar{u}\mid\Delta\tau_{F}\right)}{1-\tilde{H}_{j}^{F}\left(\tau^{*}-\tau;\bar{u}\mid\Delta\tau_{F}\right)}\prod_{\substack{G\in A'\\G\neq F}}\frac{1-\tilde{H}_{j}^{G}\left(t-\tau;\bar{u}\mid\Delta\tau_{F}\right)}{1-\tilde{H}_{j}^{G}\left(\tau^{*}-\tau;\bar{u}\mid\Delta\tau_{F}\right)}\prod_{H\notin A'}\frac{1-F_{j}^{H}\left(t-\tau;\bar{u}\right)}{1-F_{j}^{H}\left(\tau^{*}-\tau;\bar{u}\right)}$$

(15)

which could be literally read as follows:

'*The ingoing density in dynamics i at point* $\bar{x}$ *and time t, with a set A of stimuli activated at time* $\bar{\tau}_A$ *and remaining activated after entering the new configuration i is equal to the sum over all the possible sets A' of activated stimuli which contain A, over all the stimuli of A' that are deactivated within the transition (*$\delta_{ji}^{F}\left(A'\rightarrow A\right)$*), over all the possible configurations j in which the already activated stimulus F induces the transition j→ i, of the* ***probability that transition j→ i induced by F occurs****, without occurring any other transition induced by stimuli* $G\in A'$ *different from F and without being activated any other stimulus* $H\notin A'$*,* ***times the probability of being in configuration j before t****, either if the previous event was the entry in dynamics j or if it was any of the stimulus activations of* $G\in A'$ *that took place in j, integrated over all the possible activation times* $\bar{\tau}_{A'/A}$ *of stimuli being deactivated after the transition, over all the possible times* τ *of entering in configuration j, over all the possible times* τ^* *of the last event and over all the possible initial values* $\bar{u}$ *of the state vector while entering in configuration j.*'

An important remark is that probabilities of stimuli deactivating with transition $j\rightarrow i$ are not considered explicitly, because as their deactivation is assumed to be associated automatically to that transition, their probability of being deactivated in the transition is thus equal to one. The same reasoning can be applied in the sequel for generalizations considering automatic (de)activations of stimuli associated with (de)activation events.

Another important remark is that, in paper 1, all stimuli that are activated have to produce a dynamic transition, except in case that they are automatically deactivated with a dynamic event induced by another stimulus. Paper 1 does not consider deactivation events, for instance, the deactivation of a stimulus when the dynamic exits the variables region in which it was activated, although it makes some comments about that. This new consideration of (de)activation symmetry could be traduced in introducing in the term $\prod_{H\notin A'}\frac{1-F_{j}^{H}\left(t-\tau;\bar{u}\right)}{1-F_{j}^{H}\left(\tau^{*}-\tau;\bar{u}\right)}$ the stimuli belonging to the subset A.

In the draft (Labeau & Izquierdo 2005c) (in the sequel 'paper 3'), the integral equations for the ingoing density $\varphi_j\left(\bar{x},(i,I),t,\bar{\tau}_{(i,I)}\right)$ are slightly modified to account for automatic (de)activations of stimuli due to (de)activation events. This new formulation also changes the reference time to which all event times are referred: in paper 1, t was set to zero for every new dynamic event, and all other (de)activation events within dynamics j were referred to τ_j, whereas in paper 3 all events (both dynamic and (de)activation events) are referred to the beginning of the transient. Said this, the integral equation for the ingoing density due to a dynamic event is:

$$\varphi\left(\bar{x},(i,I),t,\bar{\tau}_{(i,I)}\right)=\sum_{(j,J)\neq(i,I)}\int_0^t d\tau\int d\bar{u}\int_0^\tau d\tau_j\left(\prod_G\int_0^\tau d\tau_G^J\right)\delta\left(\bar{x}-\bar{g}_j\left(t-\tau,\bar{u}\right)\right)$$
$$\times\left[\pi\left(\bar{u},(j,J),\tau\right)\delta(\tau)\delta_{J,I_0}\delta\left(\bar{\tau}_{(j,J)}\right)+\varphi\left(\bar{u},(j,J),\tau,\bar{\tau}_{(j,J)}\right)\right]Q_{ji}^{JI}\left(t,\bar{\tau}_{(i,I)};\tau,\bar{u},\bar{\tau}_{(j,J)}\right) \quad (16)$$

where $Q_{ji}^{JI}\left(t,\bar{\tau}_{(i,I)};\tau,\bar{u},\bar{\tau}_{(j,J)}\right)$ is the probability kernel analogue to $p_{ji}^{F}\left(t;\tau^*,\tau,\bar{u},\bar{\tau}_{A'},A'\right)$ in equation (14).

Figure 9 displays schematically how the branching process within a sequence is treated in this framework: entering in dynamics *j* at time τ_j, and being the last event the (de)activation of stimulus *G* at time $\tau=\tau_G^J$, we may have at time *t* whether a dynamic event, inducing a new dynamic configuration *i* or a (de)activation event, both with their respective associated automatic (de)activations of other stimuli, yielding to a new stimuli configuration *I*.

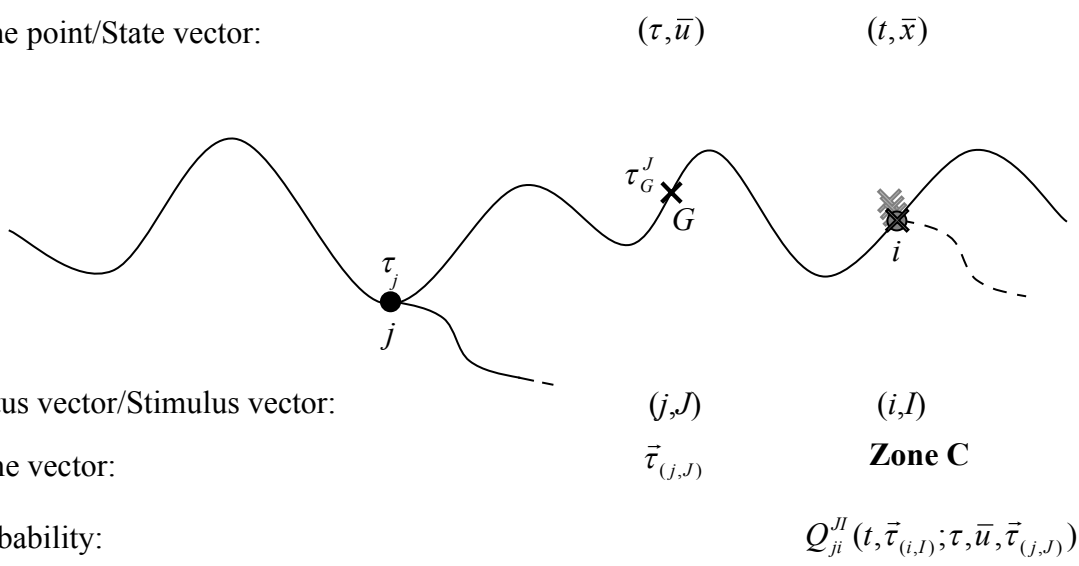


Figure 9: Event tree branching process within the SDTPD framework.

5.2 New formulation for the 'paths and sequences' SDTPD

The integral equations of the ingoing density $\varphi_{ET}^{n}\left(\bar{x}_n,(j_n,I),t,\vec{\tau}_{(j_n,I)}\right)$ in the 'paths and sequences' approach can be used to compute the figure of merit of the exceedance frequency to a given damage *D* of type *p*, $v^{exc}\left(D_p\right)$, used in the classical PSA. The original formulation of this approach is the following:

$$v^{exc}\left(D_p\right)\equiv\lim_{t\to\infty}\sum_{n,\vec{j}_n,I}\int d\vec{\tau}_{(j_n,I)}\varphi_{ET}^{n}\left(\bar{x}_n,\left(j_n,I\right),t,\vec{\tau}_{(j_n,I)}\right)\theta\left(\int_0^t d\tau DG_p\left(\bar{u}_{\vec{j}_n}\left(\vec{\tau},\vec{\tau}_{j_n}\right)\right)-D_p\right) \tag{17}$$

$$\varphi_{ET}^{n}\left(\bar{x}_n,\left(j_n,I\right),t,\vec{\tau}_{(j_n,I)}\right)=\sum_I\int_0^{\tau_{j_n}}d\tau_{j_{n-1}}\int_{\tau_{j_{n-1}}}^{t}d\tau\left(\prod_G\int_0^{\tau}d\tau_G^I\right)\left[\varphi_{ET}^{n}\left(\bar{u}_n,\left(j_n,J\right),\tau,\vec{\tau}_{(j_n,J)}\right)Q_{j_n,j_n}^{JI}\left(t,\vec{\tau}_{(j_n,I)};\tau,\bar{u}_n,\vec{\tau}_{(j_n,J)}\right)+\varphi_{dyn}^{n-1}\left(\hat{\bar{u}}_n,\left(j_{n-1},J\right),\tau,\vec{\tau}_{(j_{n-1},J)}\right)Q_{j_{n-1},j_n}^{JI}\left(t,\vec{\tau}_{(j_n,I)};\tau,\hat{\bar{u}}_n,\vec{\tau}_{(j_{n-1},J)}\right)\right] \tag{18}$$

$$Q_{j_n,j_n}^{JI}\left(t,\tau,\bar{u}_n,\vec{\tau}_{(j_n,J)},\vec{\tau}_{(j_n,I)}\right)=\delta_{j_n,j_n}\delta\left(\tau_{j_n}-\tau_{j_n}\right)\sum_G\widetilde{Q}_{j_n}^{J,G}\left(t,\tau,\bar{u}_n,\vec{\tau}_{(j_n,J)}\right)\Omega_{j_n}^{G}\left(J\to I\right)\prod_{F\in A_G\left(j_n,J\right)}\delta\left(t-\tau_F^I\right)\prod_{H\notin A_G\left(j_n,J\right)}\delta\left(\tau_H^J-\tau_H^I\right) \tag{19}$$

$$\widetilde{Q}_{j_n}^{J,G}\left(t,\tau,\bar{u}_n,\vec{\tau}_{(j_n,J)}\right)=\widetilde{f}_{(j_n,J)}^{G_{JI}}\left(t-\tau;\bar{u}_n\mid\tau-\tau_{G_{JI}}^{J}\right)\prod_{G\neq G_{JI}}\left(1-\widetilde{F}_{(j_n,J)}^{G}\left(t-\tau;\bar{u}_n\mid\tau-\tau_G^J\right)\right)\prod_{Fs.t.J_F=+}\frac{1-\widetilde{H}_{j_n}^{F}\left(t-\tau_{j_n};\bar{u}_{j_n}\mid\tau_{j_n}-\tau_F^J\right)}{1-\widetilde{H}_{(j_n,J)}^{G}\left(t-\tau_{j_n};\bar{u}_{j_n}\mid\tau_{j_n}-\tau_F^J\right)} \tag{20}$$

$$\widetilde{f}_{(j_n,J)}^{G_{JI}}\left(t-\tau;\bar{u}_n\mid\tau-\tau_{G_{JI}}^{J}\right)=\frac{f_{(j_n,J)}^{G_{JI}}\left(t-\tau_{G_{JI}}^{J};\bar{u}_{j_n}^{G_{JI}}\right)}{1-F_{(j_n,J)}^{G_{JI}}\left(\tau-\tau_{G_{JI}}^{J};\bar{u}_{j_n}^{G_{JI}}\right)} \tag{21}$$

$$f_{(j_n,J)}^{G_{JI}}\left(t-\tau_{G_{JI}}^{J};\bar{u}_{j_n}^{G_{JI}}\right)=q_{M1}^{G_{JI}}\delta\left(t-\tau_{(j_n,J),1}^{G_{JI}}\left(\bar{u}_{j_n}^{G_{JI}}\right)\right)+\left(1-q_{M1}^{G_{JI}}\right)q_{M2}^{G_{JI}}\delta\left(t-\tau_{(j_n,J),2}^{G_{JI}}\left(\bar{u}_{j_n}^{G_{JI}}\right)\right)+\ldots+\prod_{k=1}^{N_M-1}\left(1-q_{Mk}^{G_{JI}}\right)q_{N_M}^{G_{JI}}\delta\left(t-t_{AD}\right) \tag{22}$$

$$Q_{j_{n-1},j_n}^{JI}\left(t,\tau,\bar{u}_n,\vec{\tau}_{(j_{n-1},J)},\vec{\tau}_{(j_n,I)}\right)=\left(1-\delta_{j_{n-1},j_n}\right)\hat{Q}_{j_{n-1},j_n}^{J}\left(t,\tau,\bar{u}_n,\vec{\tau}_{(j_{n-1},J)}\right)\Omega_{j_{n-1},j_n}\left(J\to I\right)\delta\left(t-\tau_{j_n}\right)\prod_{G\in\left\{G_{j_{n-1},j_n}\right\}}\delta\left(t-\tau_G^I\right)\prod_{H\notin\left\{G_{j_{n-1},j_n}\right\}}\delta\left(\tau_H^I-\tau_H^J\right) \tag{23}$$

$$\hat{Q}_{j_{n-1},j_n}^{J}\left(t,\tau,\bar{u}_{n-1},\vec{\tau}_{(j_{n-1},J)}\right)=\sum_{Gs.t.J_G=+}\frac{\widetilde{h}_{j_{n-1},j_n}^{G}\left(t-\tau_{j_{n-1}};\bar{u}_{j_{n-1}}\mid\tau_{j_{n-1}}-\tau_G^J\right)}{1-\widetilde{H}_{j_{n-1}}^{G}\left(\tau-\tau_{j_{n-1}};\bar{u}_{j_{n-1}}\mid\tau_{j_{n-1}}-\tau_G^J\right)}\prod_{\substack{Fs.t.J_F=+\\F\neq G}}\frac{1-\widetilde{H}_{j_{n-1}}^{F}\left(t-\tau_{j_{n-1}};\bar{u}_{j_{n-1}}\mid\tau_{j_{n-1}}-\tau_F^J\right)}{1-\widetilde{H}_{j_{n-1}}^{F}\left(\tau-\tau_{j_{n-1}};\bar{u}_{j_{n-1}}\mid\tau_{j_{n-1}}-\tau_F^J\right)}\prod_H\left(1-\widetilde{F}_{(j_{n-1},J)}^{H}\left(t-\tau;\bar{u}_{n-1}\mid\tau-\tau_H^J\right)\right) \tag{24}$$

$$\widetilde{h}^{G}_{j_{n-1},j_n}\left(t-\tau_{j_{n-1}};\bar{u}_{j_{n-1}} \mid \tau_{j_{n-1}}-\tau^{J}_{G}\right)=\frac{h^{G}_{j_{n-1},j_n}\left(t-\tau^{J}_{G};\bar{u}^{G}_{j_n}\right)}{1-H^{G}_{j_{n-}}\left(\tau_{j_{n-1}}-\tau^{J}_{G};\bar{u}^{G}_{j_n}\right)} \tag{25}$$

$$h^{G}_{j_{n-1},j_n}\left(t-\tau^{J}_{G};\bar{u}^{G}_{j_{n-1}}\right)=q^{G}_{M1}h(t) \tag{26}$$

Several comments can be made to this formulation:

- Delay functions $\widetilde{h}$ are defined in the original paper 1 (eq. (26)) as renormalized functions accounting for two different aspects of the problem at the same time: first, the fact that the function h_j^{F} itself may change from one dynamic interval to the following, so we have to renormalize it for each interval; and second, the conditioning of probabilities of those stimuli that were activated before the dynamic change to survive up to that moment. However, in this generalisation, activation functions $\widetilde{f}$ are defined just with the conditioning of probabilities, and equation for $\widetilde{Q}_{j_n}^{J,G}$ is not clear about the subgroups of stimuli covered by each product operator.
- Boolean Ω matrices express a Boolean operation changing the state of those stimuli associated to a given (de)activation or transition event, which are not the 'driving stimulus', i.e., the one being (de)activated or inducing the dynamic transition. In the main diagonal there would be ones, indicating the change of status of the 'driving' or 'father stimulus', and off the diagonal would be ones in those stimuli also changing of status with the (de)activation of the 'father', and zero otherwise. There may be defined one matrix for the activation event and other different one for the deactivation event. However, this matrix should not be inside the ingoing density equation, as it acts over the stimuli vector *J*, and not over the probabilities.
- The sum over all the stimuli *G* in the (de)activation events should be only extended to the subgroup of stimuli changing of state in this transition, i.e., $G \in \{A_G\}$. This sum means that we can arrive to state *I* by considering any of the *G*'s of this subgroup to be the 'father' stimulus, the other changing due to the Ω matrix, so we have to add up all the probabilities of those different possibilities.
- Differently, in a dynamic transition, even if there may be several stimuli changing of state, if we assume that a unique 'father' can induce that transition, no sum over those stimuli has to be taken into account for the probabilities, as they are only affected by the Boolean function Ω. However, if we consider that may exist more than one stimulus driving that specific dynamic transition, then we have to sum up all the possibilities, i.e., over all the stimuli that were initially activated from those changing of state in that transition. In that sense, the sum appearing in the expression of $\hat{Q}^{J}_{j_{n-1},j_n}\left(t,\tau,\bar{u}_{n-1},\vec{\tau}_{(j_{n-1},J)}\right)$ should be reduced to those activated stimuli that change of state whithin the transition.
- The two terms of the equation for the ingoing density $\varphi^{n}_{ET}\left(\bar{x}_n,(j_n,I),t,\vec{\tau}_{(j_n,I)}\right)$, corresponding respectively to activation events and dynamic events have many similarities. They can, therefore, be formulated with the same generic expression, that would explicitly take into account the differences between them. The most important difference is that dynamic events have to update the sojourn time τ_{jn}, whereas activation events only update the reference times of the corresponding (dis)activated stimuli, τ_G^J. The second important difference is that dynamic events probability has to account for the probability of the corresponding activated stimulus not being disactivated before the dynamic transition.

With all those comments and suggestions, we propose the following compacted formulation of the ingoing density (entering in the damage exceedance frequency equation):

$$v^{exc}\left(D_p\right)\equiv\lim_{t\to\infty}\sum_{n,\vec{j}_n,I}\int d\vec{\tau}_{(i,I)}\varphi^n\left(\bar{x}_i,(i,I),t,\vec{\tau}_{(i,I)}\right)\theta\left(\int_0^t d\vec{\tau}DG_p\left(\bar{u}_{\vec{j}_n}\left(\vec{\tau},\vec{\tau}_i\right)\right)-D_p\right) \tag{27}$$

$$\varphi^n\left(\bar{x}_i,(i,I),t,\vec{\tau}_{(i,I)}\right)=\sum_{(j,J)\neq(i,I)}\int_0^{\tau_i}d\tau_j\int_{\tau_j}^t d\tau\left(\prod_G\int_0^{\tau}d\tau_G^J\right)\left[\varphi^{n+\delta_{ji}-1}\left(\bar{u}_j,(j,J),\tau,\vec{\tau}_{(j,J)}\right)Q_{ji}^{JI}\left(t,\vec{\tau}_{(i,I)};\tau,\bar{u}_j,\vec{\tau}_{(j,J)}\right)\right] \tag{28}$$

$$Q_{ji}^{JI}\left(t,\tau,\bar{u}_n,\vec{\tau}_{(j,J)},\vec{\tau}_{(i,I)}\right)=\left(\delta_{ji}\delta\left(\tau_j-\tau_i\right)+\left(1-\delta_{ji}\right)\delta\left(t-\tau_i\right)\right)\times$$
$$\times\sum_G\widetilde{Q}_j^{J,G}\left(t,\tau,\bar{u}_j,\vec{\tau}_{(j,J)}\right)\cdot\left|\Omega_{G,G}^{ji}\left(J\to I\right)\right|\prod_{R\in\left\{G_{ji}^{JI}\right\}}\delta\left(t-\tau_R^I\right)\prod_{S\notin\left\{G_{ji}^{JI}\right\}}\delta\left(\tau_S^J-\tau_S^I\right) \tag{29}$$

$$\widetilde{Q}_j^{J,G}\left(t,\tau,\bar{u}_j,\vec{\tau}_{(j,J)}\right)=\widetilde{g}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)\prod_{S\neq G}\left(1-\widetilde{F}_{(j,J)}^S\left(t-\tau;\bar{u}_j\mid\tau-\tau_S^J\right)\right)\prod_{\substack{T\in\left\{G^+\right\}\\T\neq G_{ji}}}\left(1-\widetilde{H}_{(j,J)}^T\left(t-\tau;\bar{u}_j\mid\tau-\tau_T^J\right)\right) \tag{30}$$

$$\widetilde{g}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)=\delta_{ji}\widetilde{f}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)+J_G\left(1-\delta_{ji}\right)\widetilde{h}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)\left(1-\widetilde{F}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)\right) \tag{31}$$

$$\widetilde{f}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)=\frac{\widetilde{f}_{(j,J)}^G\left(t-\tau_G^J;\bar{u}_j^G\right)}{1-\widetilde{F}_{(j,J)}^G\left(\tau-\tau_G^J;\bar{u}_j^G\right)}\qquad\widetilde{h}_{(j,J)}^G\left(t-\tau;\bar{u}_j\mid\tau-\tau_G^J\right)=\frac{\widetilde{h}_j^G\left(t-\tau_G^J;\bar{u}_j^G\right)}{1-\widetilde{H}_j^G\left(\tau-\tau_G^J;\bar{u}_j^G\right)} \tag{32,33}$$

$$\widetilde{h}_j^G\left(t-\tau_G^J;\bar{u}_j^G\right)=q_{M1}^G h(t) \tag{34}$$

$$\widetilde{f}_{(j,J)}^G\left(t-\tau_G^J;\bar{u}_j^G\right)=q_{j,M1}^G\delta\left(t-\tau_{j,M1}^G\left(\bar{u}_j^G\right)\right)\cdot\theta\left(\tau_{j,M1}^G\left(\bar{u}_j^G\right)-\tau_G^J\right)\cdot\theta\left(\tau_{j,M1}^G\left(\bar{u}_j^G\right)-\tau\right)+$$
$$+\left(1-q_{j,M1}^G\right)q_{j,M2}^G\delta\left(t-\tau_{j,M2}^G\left(\bar{u}_j^G\right)\right)\cdot\theta\left(\tau_{j,M2}^G\left(\bar{u}_j^G\right)-\tau_{j,M1}^G\left(\bar{u}_j^G\right)\right)\cdot\theta\left(\tau_{j,M2}^G\left(\bar{u}_j^G\right)-\tau\right)+\ldots$$
$$\ldots+\prod_{k=1}^{N_M-1}\left(1-q_{j,Mk}^G\right)q_{j,N_M}^G\delta\left(t-t_{AD}\right) \tag{35}$$

where J_G is the G^{th} component of the stimuli vector J. Probabilities $q_{Mi}{}^G$ are activation probabilities if $G\in\{G^-\}$ and deactivation probabilities if $G\in\{G^+\}$. In Dirac's delta $\delta\left(t-\tau_{j,M}^G\right)$, $\tau_{j,M}^G$ is the absolute time in which the setpoint of region M is crossed, and could be expressed as $\tau_{j,M}^G=\tau_j+\Delta\tau_{j,M}^G$ if necessary, the last being the setpoint crossing time elapsed since the time τ_j in which the system entered into dynamics j. This formulation has to be combined with the Boolean functions Ω_{ji}^{JI}, which change the stimuli vector from state J to state I on each transition j to i, either if $j=i$ (activation event) or not (dynamic event).

5.3 Definition of the Ω matrices

The Ω matrices define the relationship among stimuli when (de)activation or dynamic events induce additional (de)activations of other stimuli. In that sense, we need

to define three different Ω matrices: the first one for activation events, the second one for deactivation events and the third one for dynamic events. They are Boolean signed matrices N_J x N_J , being N_J the dimension of the stimuli vector *J*. The main diagonal corresponds to the 'father' stimulus inducing the (de)activation event, and the off-diagonal elements are the rest of the stimuli. Value 1 indicates activation of a stimulus, value -1 indicates deactivation and value 0 indicates no change on the state of the stimulus. In general, activation matrices will contain ones in the main diagonal, deactivation matrices will contain minus ones and dynamic matrices will contain minus ones (a dynamic transition normally leads to the deactivation of the corresponding 'father' stimulus) and zeros (if the stimulus being considered cannot lead to the dynamic transition $j \to i$). All those matrices are usually sparse.

In general, each dynamic state *j* is characterized by its own activation and (de)activation matrices, $\Omega^{j,act}$ and $\Omega^{j,deact}$ (for (de)activation events within dynamics *j*), and each transition $j \to i$ by its own dynamic matrix, Ω^{ji}.

An example for $N_J = 5$ is given below:

$$\Omega^{j,act} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{36}$$

In this example, activation of stimulus 1 would activate automatically stimulus 4 and 5, leaving unchanged the rest of stimuli; activation of stimulus 2 would deactivate stimulus 3, and so on.

Let us note that matrices may be non-symmetric with respect to associated (de)activations, i.e., the activation of a given 'father' stimulus leading to the activation of another one does not necessarily imply that considering the second one as 'father' will also lead to the activation of the first one. This fact is reflected on the computation of the probabilities Q_{ji}^{JI} for (de)activation events (eq. 29), reducing the sum of $\widetilde{Q}_j^{J,G}$ over all *G* to the subset of stimuli whose consideration as 'father' leads to the transition from state *J* to *I*. This reduction is done when multiplying the sum over all *G* by the absolute value of $\Omega_{G,G}^{ji}(J \to I)$ (see eq. 29), which is defined as the G^{th} diagonal element of Ω for those stimuli *G* 'leading' (as father) to the transition $J \to I$. If $j \neq i$, then $\Omega_{G,G}^{ji}(J \to I)$ is taken from the dynamic matrix Ω^{ji}, and if $j=i$ then $\Omega_{G,G}^{ji}(J \to I)$ must be taken from the activation or the deactivation matrix, $\Omega^{j,act}$ and $\Omega^{j,deact}$, depending whether if stimulus *G* is activated or deactivated in the transition $J \to I$ respectively.

In the example, the activation of stimulus 1 leads to two additional activations (stimuli 4 and 5), but only the consideration of stimulus 5 as father leads to the same final activation state *I*, as it also activates stimuli 1 and 4. This does not occur, however, when considering stimulus 4 as father, because its activation leads to the deactivation of stimulus 2, which is a completely different final state *I* than the one being considered.

Therefore, in this case, although $\{G_{ji}^{JI}\}=\{1,4,5\}$, the sum over all G would be reduced to the subset of stimuli $\{1,5\}\subset\{G_{ji}^{JI}\}$. This corresponds to only consider the terms $\Omega_{1,1}^{j,act}$ and $\Omega_{5,5}^{j,act}$ in the sum. The same remark can be made in the case of dynamic events, in which the sum is already reduced (through the term J_G in the computation of $\tilde{g}_{(j,J)}^{G}$) to the subset $G\in\{G^{+}\}$, but has to be further reduced to the subset of those activated stimuli whose 'father' consideration for the dynamic transition also leads to the transition $J\to I$ in the stimuli vector.

In practice, to find the possible "fathers" of a given transition $J \to I$, we must substract from the stimuli state vector I each row of the corresponding Ω matrix, to get G possible previous states leading to I. The ones coinciding with the real previous state J will yield to the stimuli that can lead to the transition $J \to I$.

5.4 Renormalizing and conditioning of functions *f* and *h*

Functions f and h are probability density functions (pdf) expressing the delay time in the stimuli (de)activation and the dynamic events occurrence respectively. In general, when an stimulus G changes of state at a given time $\tau_G{}^J$, (de)activation delay starts accounting for the next change of state, defined by the pdf f_G. Additionally, if the change of state was an activation event, then dynamic delay will also start accounting for the occurrence of the dynamic transition, defined by the pdf h_G.

As many other (de)activation or dynamic events may occur in between, due to other stimuli, the survival of the pdf's f_G and h_G through all those other changes has to be taken into account for probability calculation purposes, i.e., the next (de)activation or dynamic event associated to stimulus G has to be ***conditioned*** to 'survive' to all the (de)activations or dynamic events occurring after its last change of state. The conditioning operation is defined as follows:

$$f_{(j,J)}^{G}\left(t-\tau;\bar{u}_j \mid \tau-\tau_G^J\right)=\frac{f_{(j,J)}^{G}\left(t-\tau_G^J;\bar{u}_j^G\right)}{1-F_{(j,J)}^{G}\left(\tau-\tau_G^J;\bar{u}_j^G\right)} \tag{37}$$

where the (de)activation probability of G at time t, $f_{(j,J)}^{G}$, starts accounting in $\tau_G{}^J$ and survives up to τ without occurring, being $F_{(j,J)}^{G}\left(\tau-\tau_G^J;\bar{u}_j^G\right)$ the cumulative density function ('cdf') from $\tau_G{}^J$ to τ. In the SDTPD formulation, conditioning is applied in equations (32) and (33).

On the other hand, probability density functions of stimulus G may change when other (de)activation or dynamic events occur, or even due to dynamic variables dependencies. For instance, the H_2 combustion probability may increase for different regions of hydrogen concentration. In this case, a ***renormalization*** of the pdf is also necessary for probability computation purposes. In the SDTPD formulation, renormalization is denoted as $\tilde{f}$ and $\tilde{h}$. Thus, definitions of f and h in equations (34) and (35) assume they are already renormalized.

Figures 10 and 11 show the effect of the conditioning operation. Original pdf's are showed in gray color, and conditioned pdf's are showed in dark color and are denoted as $\hat{f}$. Some remarks have to be made:

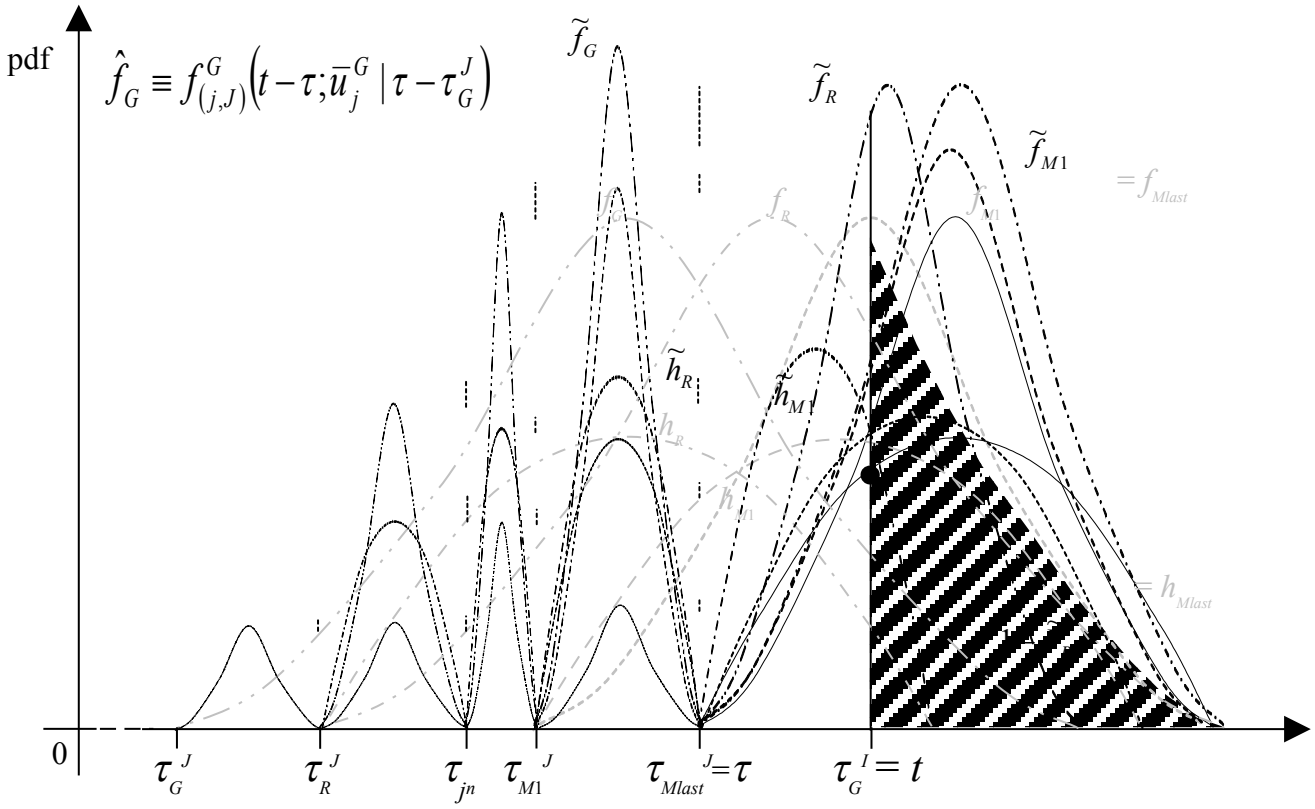


Figure 10: Conditioning of *f* and *h* functions to survive up to each event time.

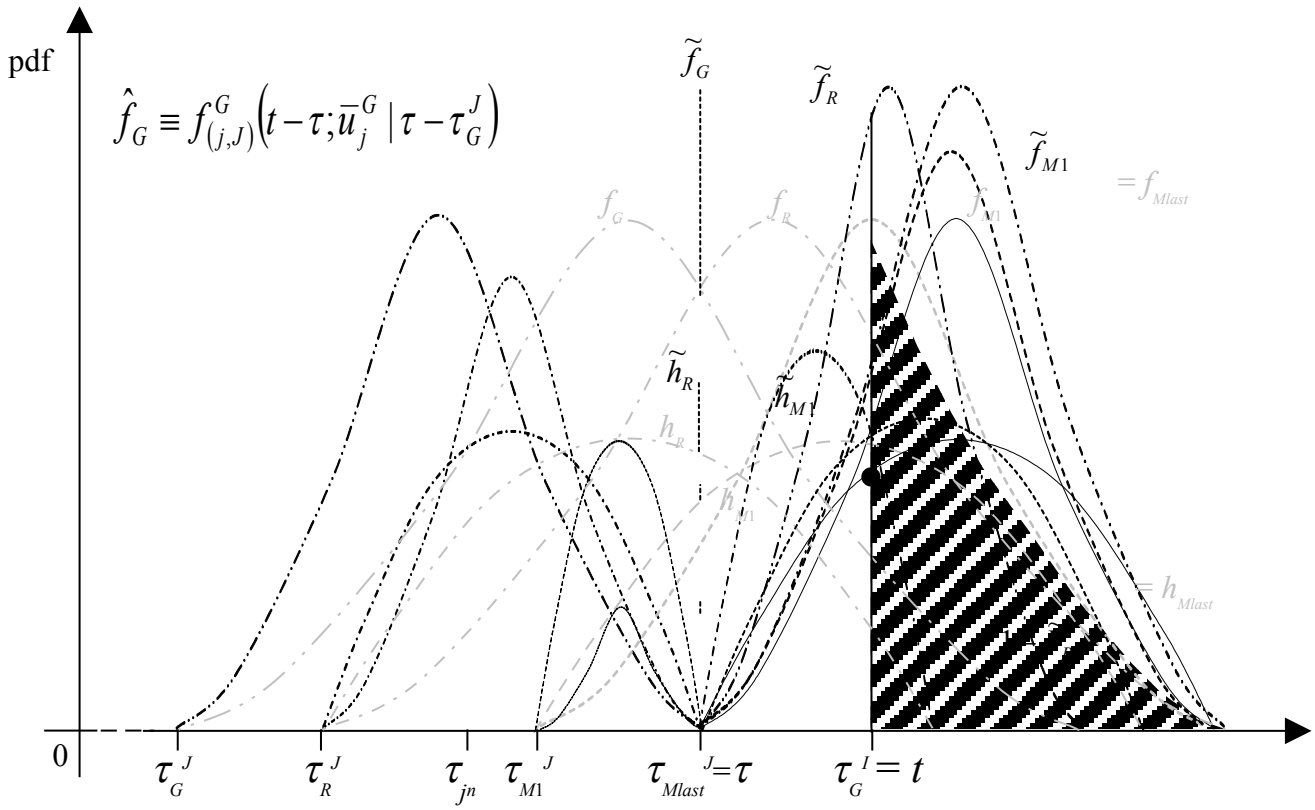


Figure 11: Conditioning of *f* and *h* functions to survive up to the last event time τ.

- If *f* and *h* functions do not change between event intervals (no renormalization), then successive conditioning for each event time (Figure 10) becomes equivalent to just conditioning for the last event time τ (Figure 11).
- If activation events are driven by setpoints or regions crossed by the dynamic variables, *f* functions shrink up to Dirac's deltas $\delta(t-\tau_{sp})$, being τ_{sp} the time in which the setpoint is crossed, later than the time of the last change of status of *G*, τ_G^J. In this case, neither renormalization nor conditioning is necessary since the activation time is instantaneous and is already specified by the setpoint.
- In the figures, *h* functions only apply at time τ_G^J for stimulus *G* if the last change of status was an activation event.

5.5 Elimination of the dependence on τ_G^I

To be able to afford the numerical resolution of the ingoing density equation, it is necessary to eliminate explicit dependencies in some variables, in order to reduce as much as possible the degrees of freedom of the equation. However, this elimination should be done as much analytical as possible, for not to lose any general character or accuracy in the application of the equations. The 'paths and sequences' approach indeed succeeded in the reduction of the dependency on the state vector $\bar{x}$, and the corresponding integral in the ingoing density equation was eliminated. At this stage, we aim to also eliminate the dependency on the activation times τ_G^I of all the stimuli *G*.

The setpoints triggering the activation of stimuli are dynamic-dependent values of the state variables $\bar{x}$ in a given transient evolution. We define $\tau_{sp}^{J_G}$ as the absolute time necessary to cross the setpoint in which stimulus *G* is (de)activated, reaching Boolean state J_G (*Gth* component of the *J* vector). This time $\tau_{sp}^{J_G}$ thus depend on the dynamics, what can be explicitly expressed as follows: $\tau_{sp}^{J_G}\left(\bar{u}^{(1-J_G)}\left(\vec{\tau}_j\right)\right)$, where $\bar{u}^{(1-J_G)}$ is the value of the state vector in the previous change of state of stimulus *G*. Once a path is fixed, i.e., the time vector for the dynamic events occurrence $\vec{\tau}_j$ is fixed, $\bar{u}^{(1-J_G)}$ will also be determined for all *G* and $\tau_{sp}^{J_G}$ will then become a fixed number.

With this definition for a setpoint, (de)activation pdf can be defined as:

$$\tilde{f}_{(j,J)}^{G}\left(t-\tau_G^J;\bar{u}_j^G\right)=\left(q_{act}^G\left(1-J_G\right)+q_{deact}^G J_G\right)\left[\theta\left(\tau_{sp}^{(1-J_G)}-\tau_G^J\right)\theta\left(\tau_{sp}^{(1-J_G)}-\tau\right)\delta\left(t-\tau_{sp}^{(1-J_G)}\right)\right] \tag{38}$$

where θ step functions account for the setpoint crossing time of stimulus *G* to be later than τ_G^J (previous change of state of *G*) and later than τ (last combined state change).

Similarly, (de)activation cdf $F^G_{(j,J)}\left(\tau-\tau^J_G;\bar{u}^G_j\right)=\widetilde{F}^G_{(j,J)}\left(\tau-\tau^J_G;\bar{u}^G_j\right)$ will be:

$$\begin{aligned}\widetilde{F}^G_{(j,J)}\left(\tau-\tau^J_G;\bar{u}^G_j\right)&=\int_0^\tau \widetilde{f}^G_{(j,J)}\left(t-\tau^J_G;\bar{u}^G_j\right)dt=\\&=\int_0^\tau\left(q^G_{act}\left(1-J_G\right)+q^G_{deact}J_G\right)\left[\theta\left(\tau^{(1-J_G)}_{sp}-\tau^J_G\right)\theta\left(\tau^{(1-J_G)}_{sp}-\tau\right)\delta\left(t-\tau^{(1-J_G)}_{sp}\right)\right]dt=\\&=\left(q^G_{act}\left(1-J_G\right)+q^G_{deact}J_G\right)\left[\theta\left(\tau^{(1-J_G)}_{sp}-\tau^J_G\right)\theta\left(\tau^{(1-J_G)}_{sp}-\tau\right)\theta\left(\tau-\tau^{(1-J_G)}_{sp}\right)\right]=0\end{aligned} \tag{39}$$

This means that in the particular case of *f*'s defined by setpoints, the conditioning (survival) of the function up to the last event τ is not necessary, as the activation function is a Dirac's delta occurring instantaneously at time $\tau^{(1-J_G)}_{sp}>\tau$.

In the sequel we will develop as further as possible the integrals over the stimuli and over τ in the expression of the ingoing density, just leaving unsolved the integral over τ_j, which will be eventually solved by the transmission functions theory. Let's distinguish between activation events and dynamic events.

- <u>*(De)activation events*</u>: to develop the integrals, we will just consider explicitly the terms with Dirac's deltas or Heaviside functions, grouping as Q^G all the terms containing probabilities.

The general expression for the ingoing density is:

$$\varphi^n\left(\bar{x}_i,(i,I),t,\vec{\tau}_{(i,I)}\right)=\sum_{(j,J)\neq(i,I)}\int_0^{\tau_i}d\tau_j\int_{\tau_j}^t d\tau\left(\prod_G\int_0^\tau d\tau^J_G\right)\left[\varphi^{n+\delta_{ji}-1}\left(\bar{u}_j,(j,J),\tau,\vec{\tau}_{(j,J)}\right)Q^{JI}_{ji}\left(t,\vec{\tau}_{(i,I)};\tau,\bar{u}_j,\vec{\tau}_{(j,J)}\right)\right] \tag{40}$$

For an activation event, $\varphi^{n+\delta_{ji}-1}=\varphi^n$, and Q^{JI}_{ji} contains the following terms:

$$\begin{aligned}Q^{JI}_{ji}\left(t,\vec{\tau}_{(i,I)};\tau,\bar{u}_j,\vec{\tau}_{(j,J)}\right)&=\delta\left(\tau_j-\tau_i\right)\theta\left(\tau^{(1-J_G)}_{sp}-\tau^J_G\right)\theta\left(\tau^{(1-J_G)}_{sp}-\tau\right)\delta\left(t-\tau^{(1-J_G)}_{sp}\right)\times\\&\times\prod_{R\in\left\{G^{JI}_{ji}\right\}}\delta\left(t-\tau^I_R\right)\prod_{S\notin\left\{G^{JI}_{ji}\right\}}\delta\left(\tau^J_S-\tau^I_S\right)\prod_{T\notin\left\{G^+\right\}}\left(1-H\left(\tau^J_T\right)\right)\cdot Q^G\end{aligned} \tag{41}$$

Integrating over all $\tau_G{}^J$ in eq. (3) yields to:

$$\begin{aligned}\varphi^n\left(\bar{x}_i,(i,I),t,\vec{\tau}_{(i,I)}\right)=\sum_{(j,J)\neq(i,I)}\int_0^{\tau_i}d\tau_j\int_{\tau_j}^t d\tau\Big[&\varphi^n\left(\bar{u}_j,(j,J),\tau,\vec{\tau}_{(j,J)}\right)\delta\left(\tau_j-\tau_i\right)\delta\left(t-\tau^{(1-J_G)}_{sp}\right)\cdot Q^G\times\\&\times\prod_{\substack{R\in\left\{G^{JI}_{ji}\right\}\\R\notin\left\{G^+\right\}}}\delta\left(t-\tau^I_R\right)\tau\prod_{\substack{S\notin\left\{G^{JI}_{ji}\right\}\\R\notin\left\{G^+\right\}}}\theta\left(\tau-\tau^I_S\right)\prod_{\substack{T\in\left\{G^+\right\}\\T\in\left\{G^{JI}_{ji}\right\}}}\delta\left(t-\tau^I_T\right)\left(\int_0^\tau d\tau^J_T\left(1-H\left(\tau^J_T\right)\right)\right)\prod_{\substack{U\in\left\{G^+\right\}\\U\notin\left\{G^{JI}_{ji}\right\}}}\left(1-H\left(\tau^I_U\right)\right)\Big]\end{aligned} \tag{42}$$

At this point we perform the integral over all possible $\tau_G{}^I$

$$\varphi^n(\bar{x}_i,(i,I),t,\tau_i)=\sum_{(j,J)\neq(i,I)}\int_0^{\tau_i}d\tau_j\int_{\tau_j}^{t}d\tau\left[\prod_G\int_0^t d\tau_G^I\right]\left[\varphi^n(\bar{u}_j,(j,J),\tau,\vec{\tau}_{(j,J)})\delta(\tau_j-\tau_i)\delta\left(t-\tau_{sp}^{(1-J_G)}\right)\cdot Q^G\times\right.$$

$$\left.\times\prod_{\substack{R\in\{G_{ji}^{JI}\}\\R\notin\{G^+\}}}\delta(t-\tau_R^I)\tau\prod_{\substack{S\notin\{G_{ji}^{JI}\}\\R\notin\{G^+\}}}\theta(\tau-\tau_S^I)\prod_{\substack{T\in\{G^+\}\\T\in\{G_{ji}^{JI}\}}}\delta(t-\tau_T^I)\left(\int_0^{\tau}d\tau_T^J\left(1-H(\tau_T^J)\right)\right)\prod_{\substack{U\in\{G^+\}\\U\notin\{G_{ji}^{JI}\}}}\left(1-H(\tau_U^I)\right)\right] \tag{43}$$

$$\varphi^n(\bar{x}_i,(i,I),t,\tau_i)=\sum_{(j,J)\neq(i,I)}\int_0^{\tau_i}d\tau_j\int_{\tau_j}^{t}d\tau\left[\varphi^n(\bar{u}_j,(j,J),\tau,\vec{\tau}_{(j,J)})\delta(\tau_j-\tau_i)\delta\left(t-\tau_{sp}^{(1-J_G)}\right)\cdot Q^G\times\right.$$

$$\left.\times\prod_{\substack{R\in\{G_{ji}^{JI}\}\\R\notin\{G^+\}}}\theta(t-t)\tau\prod_{\substack{S\notin\{G_{ji}^{JI}\}\\R\notin\{G^+\}}}\tau\prod_{\substack{T\in\{G^+\}\\T\in\{G_{ji}^{JI}\}}}\theta(t-t)\left(\int_0^{\tau}d\tau_T^J\left(1-H(\tau_T^J)\right)\right)\prod_{\substack{U\in\{G^+\}\\U\notin\{G_{ji}^{JI}\}}}\left(\int_0^t d\tau_T^I\left(1-H(\tau_T^I)\right)\right)\right] \tag{44}$$

Although this result may be valid, expression (5) is very complicated and new approaches will need to be done to simplify the dependency on τ_G^I in earlier stages of the ingoing density derivation.

5.6 RELATIONSHIP BETWEEN (DE)ACTIVATION PROBABILITIES: BINARY-STATE MARKOVIAN SYSTEM

A single stimulus may be seen as a Markovian system of only two states: activated and deactivated. In that sense, we have applied the classical Markov equation to determine the possible relation between the activation and deactivation probabilities (both embedded in the pdf function *f*), and their relation with the initial conditions probability.

The fundamental Markov equation is:

$$\frac{d}{dt}(\pi_j(t))=-\lambda_j(t)\cdot\pi_j(t)+\varphi_j(t) \tag{45}$$

where

$\lambda_j(t)=\sum_{k\neq j}p_{j\to k}(t)\equiv$ transition rate from state *j* to state *k*, and

$\varphi_j(t)=\sum_{k\neq j}p_{k\to j}(t)\cdot\pi_k(t)\equiv$ ingoing density from state *k* to state *j*.

If we apply equation (1) to a binary-state system, as that of a single stimulus (two possible states: activated, '+', and deactivated, '-'), we have:

$$\frac{d}{dt}(\pi_+(t))=-\lambda_+(t)\cdot\pi_+(t)+\varphi_+(t) \tag{46}$$

where

$\lambda_+(t)=p_{+\to-}(t)=p_-(t)\equiv$ deactivation probability, and

$\varphi_+(t)=p_{-\to+}(t)\cdot\pi_-(t)=p_+(t)\cdot\pi_-(t)$, being $p_+(t)\equiv$ activation probability.

So the system of equations defining the problem is set as follows:

$$\begin{cases} \dfrac{d}{dt}(\pi_+(t)) = -p_-(t)\cdot\pi_+(t) + p_+(t)\cdot\pi_-(t) \\ \dfrac{d}{dt}(\pi_-(t)) = -p_+(t)\cdot\pi_-(t) + p_-(t)\cdot\pi_+(t) \end{cases} \tag{47}$$

System of equations (47) can be written in matricial form:

$$\frac{d}{dt}\pi(t) = P(t)\cdot\pi(t) \tag{48}$$

where

$$\pi(t) = \begin{pmatrix} \pi_+(t) \\ \pi_-(t) \end{pmatrix}; \qquad P(t) = \begin{pmatrix} -p_-(t) & p_+(t) \\ p_-(t) & -p_+(t) \end{pmatrix} \tag{49}$$

The solution for this first-order system of equations is given by the Laplace transform. If we denote by $\pi^*(s)$ the Laplace transform of $\pi(t)$, then the Laplace transform of the system of eqs. (48) is:

$$s\pi^*(s) - \pi(0) = P(t)\cdot\pi^*(s) \tag{50}$$

where $\pi(0)$ is the vector of initial conditions. Let us assume that the stimulus has a probability $\pi_+(0) = \pi_0$ of being activated at t=0, thus

$$\begin{cases} s\pi_+^*(s) - \pi_0 = -p_-\cdot\pi_+^*(s) + p_+\cdot\pi_-^*(s) \\ s\pi_-^*(s) - (1-\pi_0) = -p_+\cdot\pi_-^*(s) + p_-\cdot\pi_+^*(s) \end{cases} \tag{51}$$

By summing up eqs. (51) we get:

$$s\pi_+^*(s) + s\pi_-^*(s) = 1 \tag{52}$$

Thus

$$\pi_-^*(s) = \frac{1}{s} - \pi_+^*(s) \tag{53}$$

and inserting this expression into the first equation of (51) we get:

$$s\pi_+^*(s) - \pi_0 = -p_-\cdot\pi_+^*(s) + p_+\cdot\left(\frac{1}{s} - \pi_+^*(s)\right)$$

$$s\pi_+^*(s) - \pi_0 = \frac{p_+}{s} - p_+\cdot\pi_+^*(s) - p_-\cdot\pi_+^*(s)$$

$$\pi_+^*(s) = \frac{p_+}{s}\cdot\frac{1}{(s+p_++p_-)} + \frac{\pi_0}{(s+p_++p_-)} \tag{54}$$

To find the inverse Laplace transform, we rewrite this expression as:

$$\pi_+^*(s) = \frac{p_+}{(p_++p_-)}\cdot\frac{1}{s} + \left(\pi_0 - \frac{p_+}{(p_++p_-)}\right)\cdot\frac{1}{(s+p_++p_-)} \tag{55}$$

The inverse Laplace transform of (5) is:

$$\boxed{\pi_+(t) = \frac{p_+}{(p_+ + p_-)} + \left(\pi_0 - \frac{p_+}{(p_+ + p_-)}\right) \cdot e^{-(p_+ + p_-)t}} \tag{56}$$

and knowing that $\pi_+(t) + \pi_-(t) = 1$, we obtain similarly:

$$\boxed{\pi_-(t) = \frac{p_-}{(p_+ + p_-)} - \left(\pi_0 - \frac{p_+}{(p_+ + p_-)}\right) \cdot e^{-(p_+ + p_-)t}} \tag{57}$$

Which are the solutions for the system of equations (47).

5.7 EXAMPLE OF APPLICATION OF THE SDTPD

Let us consider a very simple system in which there are two components with their corresponding stimuli. The system is compound by a containment filled with a mixture of gases and two valves: an inflow valve (V_{in}) and an outflow valve (V_{out}). The aim of these components is to keep the pressure inside the containment approximately constant and equal to P_0. However, we consider that the components behave differently: the inflow valve opens whenever the pressure of the system decreases below a given setpoint P_{min}, and closes whenever the pressure surpasses another setpoint P_{max}; and the outflow valve opens whenever the pressure increases (positive derivative of the pressure curve) and closes whenever the pressure decreases (negative derivative). All those transition events are assumed to occur with a given delay after the corresponding stimulus activation. The damage limit is defined as a maximum permissible time, t_{lim}, for the cumulated time in which pressure in the containment is beyond the pressure interval [P_{min}, P_{max}].

There are the following possible dynamic states given by Table 1:

Components	J_{in}	J_{out}
Dynamic state 1, d_{none}	0	0
Dynamic state 2, d_{out}	0	1
Dynamic state 3, d_{in}	1	0
Dynamic state 4, d_{inout}	1	1

Table 1: Possible dynamic states of the two-valves example.

The status vector is, therefore, $J = (J_{in}, J_{out})$, and indicates the status of the V_{in} and V_{out} valves. The stimuli vector will be $I = (I_{Oin}, I_{Cin}, I_{Oout}, I_{Cout}, I_D)$, whose components are associated to open and close V_{in} and open and close V_{out} respectively. The last stimulus indicates when the damage limit has been surpassed. Possible transitions between dynamic states are showed in Figure 12:

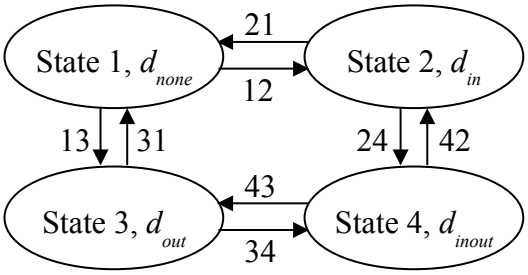
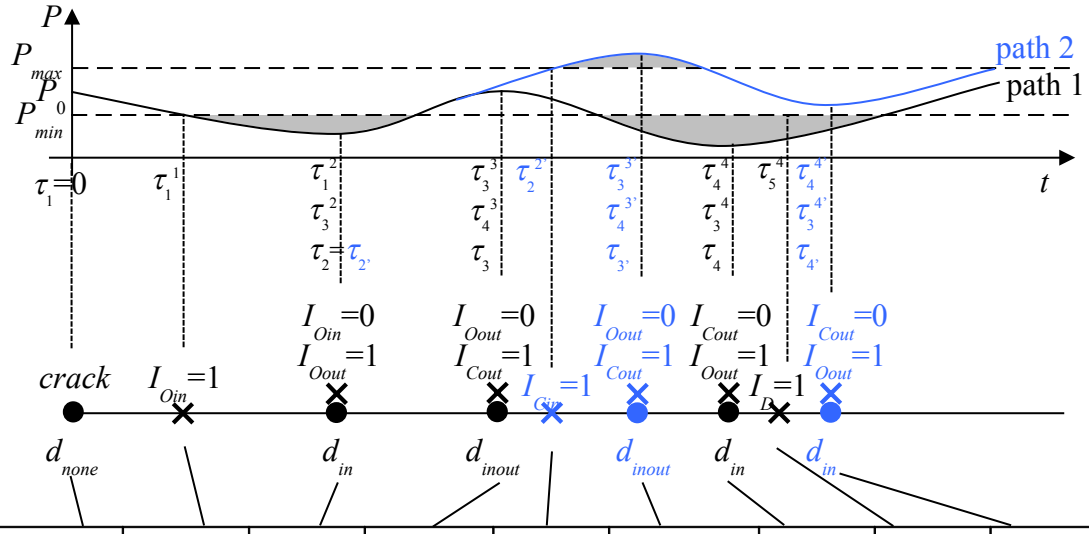


Figure 12: Possible transition between states.

Transition events (dis)activating a particular component instantaneously disactivate the corresponding stimulus. Additionally, some stimuli can be (dis)activated automatically with the (dis)activation of other stimuli/components.

The initiating event for this example will be a crack in the containment, promoting the gases inside the containment to escape and therefore the pressure starts decreasing. Figure 13 shows two posible paths for a given sequence. The first one ends with damage and the second one does not. We will just compute the exceedance

frequency of that sequence considering only those two paths for simplicity (although there may be much more paths in the same sequence). Table 2 presents the state of all associated vectors on each transition point.



Dynamic state, j_k	j_1 (none)	j_1 (none)	j_2 (in)	j_3 (inout)	j_2' (in)	j_3' (inout)	j_4 (in)	j_4 (in)	j_4' (in)
Stimuli state, J_k	J_0	J_1	J_2	J_3	J_3'	J_4'	J_4	J_5	J_5'
Initial state vector (u=P)	P_0	P_{min}	$P< P_{min}$	$P> P_{min}$ $P< P_{max}$	P_{max}	$P>P_{max}$	$P< P_{min}$	$P< P_{min}$	$P> P_{min}$ $P< P_{max}$
Status vector (J)	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$
Stimuli vector (I)	$\begin{bmatrix}0\\0\\0\\0\\0\end{bmatrix}$	$\begin{bmatrix}1\\0\\0\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\\0\\1\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\\1\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\\0\\1\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\\1\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\0\\1\\0\\1\end{bmatrix}$	$\begin{bmatrix}0\\1\\1\\0\\0\end{bmatrix}$
Time vector ($\vec{\tau}$)	$\begin{bmatrix}0\\0\\0\\0\\0\\0\end{bmatrix}$	$\begin{bmatrix}0\\\tau_1^{J_1}\\0\\0\\0\\0\end{bmatrix}$	$\begin{bmatrix}\tau_2\\\tau_1^{J_2}\\0\\\tau_3^{J_2}\\0\end{bmatrix}$	$\begin{bmatrix}\tau_3\\\tau_1^{J_2}\\0\\\tau_3^{J_3}\\\tau_4^{J_3}\end{bmatrix}$	$\begin{bmatrix}\tau_{2'}\\\tau_1^{J_2}\\\tau_2^{J_3'}\\\tau_3^{J_2}\\0\end{bmatrix}$	$\begin{bmatrix}\tau_{3'}\\\tau_1^{J_2}\\\tau_2^{J_3'}\\\tau_3^{J_4'}\\\tau_4^{J_4'}\end{bmatrix}$	$\begin{bmatrix}\tau_4\\\tau_1^{J_2}\\0\\\tau_3^{J_4}\\\tau_4^{J_4}\end{bmatrix}$	$\begin{bmatrix}\tau_4\\\tau_1^{J_2}\\0\\\tau_3^{J_4}\\\tau_4^{J_4}\end{bmatrix}$	$\begin{bmatrix}\tau_{4'}\\\tau_1^{J_2}\\\tau_2^{J_3'}\\\tau_3^{J_5'}\\\tau_4^{J_5'}\end{bmatrix}$
Activation/ transition event (n)	0	1	0 2	0 3	0 3'	0 4'	0 4	$\tau_5^{J_5}$ 5	0 5'

Figure 13 and Table 2: Example of two paths of the same sequence, with all the associated vectors for each transition point.

Let us calculate now the ingoing density for each of the activation/transition instants n (each column in the previous table). Remark than they do not coincide with the number of dynamic states, j_n, as there are events with stimuli (dis)activation, but without transition on the dynamics:

- $\underline{n = 0}$: the initiating event (containment crack) introduces the system into dynamics j_1.

$$\varphi^1\left(\bar{x}_{j_1},(j_1,J_0),t,\vec{\tau}_{(j_1,J_0)}\right)=\varphi^0\cdot q^{crack} \tag{58}$$

- $\underline{n = 1}$: the stimulus I_{Oin} is activated when crossing the setpoint P_{min}.

$$\varphi^1\left(\bar{x}_{j_1},(j_1,J_1),t,\vec{\tau}_{(j_1,J_1)}\right)=\sum_I\int_0^{\tau_1}d\tau_{j_1}\int_{\tau_1}^{t}d\tau\int_0^{\tau}d\tau_1^{J_1}\int_0^{\tau}d\tau_2^{J_1}\int_0^{\tau}d\tau_3^{J_1}\int_0^{\tau}d\tau_4^{J_1}\int_0^{\tau}d\tau_5^{J_1}\left[\varphi^1\left(\bar{u}_{j_1},(j_1,J_0),t,\vec{\tau}_{(j_1,J_0)}\right)\cdot\right.$$
$$\left.\cdot\delta\left(\tau_{j_1}-\tau_{j_1}\right)q^{Oin}\delta\left(t-\tau_{j_1,sp}^{act}(P_0)\right)\left(1-q^{Cin}\right)\left(1-q^{Oout}\right)\left(1-q^{Cout}\right)\left(1-q^{D}\right)\delta\left(\tau_2^{J_0}-\tau_2^{J_1}\right)\delta\left(\tau_3^{J_0}-\tau_3^{J_1}\right)\delta\left(\tau_4^{J_0}-\tau_4^{J_1}\right)\delta\left(\tau_5^{J_0}-\tau_5^{J_1}\right)\right] \tag{59}$$

$$Q_{j_1j_1}^{J_0J_1}\left(t,\tau,P_0,\vec{\tau}_{(j_1,J_0)},\vec{\tau}_{(j_1,J_1)}\right)=\delta\left(\tau_{j_1}-\tau_{j_1}\right)q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right)\left(1-q^{Cin}\right)\left(1-q^{Oout}\right)\left(1-q^{Cout}\right)\left(1-q^{D}\right)\cdot$$
$$\cdot\delta\left(\tau_2^{J_0}-\tau_2^{J_1}\right)\delta\left(\tau_3^{J_0}-\tau_3^{J_1}\right)\delta\left(\tau_4^{J_0}-\tau_4^{J_1}\right)\delta\left(\tau_5^{J_0}-\tau_5^{J_1}\right) \tag{60}$$

$$\widetilde{Q}_{j_1}^{J_0,Oin}\left(t,\tau,P_0,\vec{\tau}_{(j_1,J_0)}\right)=q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right)\left[\left(1-q^{Cin}\right)\left(1-q^{Oout}\right)\left(1-q^{Cout}\right)\left(1-q^{D}\right)\right] \tag{61}$$

$$\widetilde{g}_{(j_1,J_0)}^{Oin}\left(t-\tau;P_0\mid\tau-\tau_1^{J_0}\right)=(1-0)q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right)+0=q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right) \tag{62}$$

$$\widetilde{f}_{(j_1,J_0)}^{Oin}\left(t-\tau;P_0\mid\tau-\tau_1^{J_0}\right)=\frac{q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right)}{1-q^{Oin}\theta\left(\tau-\tau_1^{J_0}(P_0)\right)}=q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right) \tag{63}$$

$$f_{(j_1,J_0)}^{Oin}\left(t-\tau_1^{J_0};P_0\right)=q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right)$$
$$\left(F_{(j_1,J_0)}^{Oin}\left(\tau-\tau_1^{J_0};P_0\right)=\int_0^{\tau}q^{Oin}\delta\left(t-\tau_1^{J_0}(P_0)\right)dt=q^{Oin}\theta\left(\tau-\tau_1^{J_0}(P_0)\right)=0\right) \tag{64}$$

$$\prod_{S\notin A_{ji}^{II}}\left(1-\widetilde{F}_{(j_1,J_0)}^{S}\left(t-\tau;P_0\mid\tau-\tau_S^{J_0}\right)\right)=\left(1-F_{(j_1,J_0)}^{Cin}\left(\tau-\tau_2^{J_0};P_0\right)\right)\left(1-F_{(j_1,J_0)}^{Oout}\left(\tau-\tau_3^{J_0};P_0\right)\right)\left(1-F_{(j_1,J_0)}^{Cout}\left(\tau-\tau_4^{J_0};P_0\right)\right)\left(1-F_{(j_1,J_0)}^{D}\left(\tau-\tau_5^{J_0};P_0\right)\right) \tag{65}$$

$$f_{(j_1,J_0)}^{Cin}\left(t-0;P_0\right)=q^{Cin}\delta\left(t-0\right)$$
$$\left(F_{(j_1,J_0)}^{Cin}\left(\tau-0;P_0\right)=\int_0^{\tau}q^{Oin}\delta\left(t\right)dt=q^{Cin}\theta\left(\tau\right)=q^{Cin}\right)$$

similarly,

$$F_{(j_1,J_0)}^{Oout}\left(\tau-0;P_0\right)=q^{Oout}$$
$$F_{(j_1,J_0)}^{Cout}\left(\tau-0;P_0\right)=q^{Cout}$$
$$F_{(j_1,J_0)}^{D}\left(\tau-0;P_0\right)=q^{D} \tag{66}$$

- $n = 2$: the inflow valve is opened, entering in the dynamics j_2 with the corresponding disactivation of I_{Oin} and an additional activation of I_{Oout}, because pressure gradient becomes positive.

$$\varphi^2\left(\bar{x}_{j_1},(j_2,J_2),t,\vec{\tau}_{(j_2,J_2)}\right)=\sum_I\int_0^{\tau_1}d\tau_{j_1}\int_{\tau_1}^{t}d\tau\int_0^{\tau}d\tau_1^{J_2}\int_0^{\tau}d\tau_2^{J_2}\int_0^{\tau}d\tau_3^{J_2}\int_0^{\tau}d\tau_4^{J_2}\int_0^{\tau}d\tau_5^{J_2}\left\{\varphi^1\left(\bar{u}_{j_1},(j_1,J_0),t,\vec{\tau}_{(j_1,J_0)}\right)\cdot\right.$$
$$\left.\cdot\,\delta\left(t-\tau_{j_2}\right)\delta\left(t-\tau_1^{J_2}\right)\delta\left(t-\tau_3^{J_2}\right)\delta\left(\tau_2^{J_1}-\tau_2^{J_2}\right)\delta\left(\tau_4^{J_1}-\tau_4^{J_2}\right)\delta\left(\tau_5^{J_1}-\tau_5^{J_2}\right)\tilde{h}^{Oin}_{(j_1,J_1)}\left(1-q^{Oin}\right)\left(1-q^{Cin}\right)\left(1-q^{Oout}\right)\left(1-q^{Cout}\right)\left(1-q^{D}\right)\right\} \tag{67}$$

$$Q^{J_1J_2}_{j_1j_2}\left(t,\tau,P_{\min},\vec{\tau}_{(j_1,J_1)},\vec{\tau}_{(j_2,J_2)}\right)=\delta\left(t-\tau_{j_2}\right)\delta\left(t-\tau_1^{J_2}\right)\delta\left(t-\tau_3^{J_2}\right)\delta\left(\tau_2^{J_1}-\tau_2^{J_2}\right)\delta\left(\tau_4^{J_1}-\tau_4^{J_2}\right)\delta\left(\tau_5^{J_1}-\tau_5^{J_2}\right)\cdot$$
$$\cdot\,\tilde{h}^{Oin}_{(j_1,J_1)}\left(1-q^{Oin}\right)\left(1-q^{Cin}\right)\left(1-q^{Oout}\right)\left(1-q^{Cout}\right)\left(1-q^{D}\right) \tag{68}$$

$$\tilde{Q}^{J_1,Oin}_{j_1}\left(t,\tau,P_{\min},\vec{\tau}_{(j_1,J_1)}\right)=\tilde{h}^{Oin}_{(j_1,J_1)}\left(t-\tau;P_{\min}\mid\tau-\tau_1^{J_1}\right)\left(1-q^{Oin}\right)\left[\left(1-q^{Cin}\right)\left(1-q^{Cout}\right)\left(1-q^{D}\right)\right] \tag{69}$$

$$\tilde{g}^{Oin}_{(j_1,J_1)}\left(t-\tau;P_{\min}\mid\tau-\tau_1^{J_1}\right)=0+1\cdot\tilde{h}^{Oin}_{(j_1,J_1)}\left(t-\tau;P_{\min}\mid\tau-\tau_1^{J_1}\right)\left(1-q^{Oin}\right) \tag{70}$$

$$\tilde{h}^{Oin}_{(j_1,J_1)}\left(t-\tau;P_{\min}\mid\tau-\tau_1^{J_1}\right)=\frac{\tilde{h}^{Oin}_{j_1}\left(t-\tau_1^{J_1};P_{\min}\right)}{1-\tilde{H}^{Oin}_{j_1}\left(\tau-\tau_1^{J_1};P_{\min}\right)} \tag{71}$$

$$\tilde{h}^{Oin}_{j_1}\left(t-\tau_1^{J_1};P_{\min}\right)=q^{Oin}h(t) \tag{72}$$

$$\prod_{S\notin A^{Jl}_{ji}}\left(1-\tilde{F}^{S}_{(j_1,J_1)}\left(t-\tau;\bar{u}_j\mid\tau-\tau_F^{J}\right)\right)=\left(1-F^{Cin}_{(j_1,J_1)}\left(\tau-\tau_2^{J_1};P_{\min}\right)\right)\left(1-F^{Cout}_{(j_1,J_1)}\left(\tau-\tau_4^{J_1};P_{\min}\right)\right)\left(1-F^{D}_{(j_1,J_1)}\left(\tau-\tau_5^{J_1};P_{\min}\right)\right) \tag{73}$$

$$f^{Cin}_{(j_1,J_1)}\left(t-\tau_2^{J_1};P_{\min}\right)=q^{Cin}\delta(t-0)$$
$$\left(F^{Cin}_{(j_1,J_1)}\left(\tau-\tau_2^{J_1};P_{\min}\right)=\int_0^{\tau}q^{Cin}\delta(t-0)dt=q^{Cin}\theta(\tau)=q^{Cin}\right)$$
similarly,
$$F^{Cout}_{(j_1,J_1)}\left(\tau-0;P_{\min}\right)=q^{Cout}$$
$$F^{D}_{(j_1,J_1)}\left(\tau-0;P_{\min}\right)=q^{D} \tag{74}$$

And so on with the rest of events until the end of the transient. Numerical work must still be done to solve the integrals from these initial expressions of the ingoing density.

6 Safety margins computed by the SDTPD

SDTPD provides mathematical balances to calculate the probabilities per unit time of entering states with specified stimuli activated and correlate them between themselves. In addition, they calculate the exceedance frequencies without any factorisation, the probability of the demand and the fraction of damage paths being embedded in the activation of the stimuli. Exceeding safety limits are particular cases of stimuli, as they are to fulfil any necessary condition required for them, so SDTPD has potential to compute the safety margins defined in chapter 2:

- Exceedance frequency safety margin: SDTPD is based on the activation of stimuli that promote dynamic transitions on the system during an accident evolution. Stimuli activate when some set point or state region is surpassed. In that sense, a stimulus could be defined with respect to a set point on the damage. In particular, whenever the damage limit of condition k is surpassed, the corresponding stimulus is activated and the exceedance frequency of the risk curve for that damage is computed. Once that exceedance frequency is known, the frequency safety margin can be computed.
- Damage safety margin: the third definition of damage safety margin, also made in terms of frequencies, is immediately computable by the SDTPD in the same terms than the previous exceedance frequency safety margin: stimuli can be defined associated to both the damage limit set point and a fraction φ of that limit, and differences between the corresponding exceedance frequencies can be computed when surpassing those set points in respective analyses.

7 Quantitative relationship between the PSA and the "paths and sequences" SDTPD

In traditional PSA, due consideration is given to the sequence delineation problem, i.e., finding success and damage sequences relative to the classical PSA safety objectives (safety limits of severe core damage and LERF). As indicated before, consideration of a sequence implies the assumption that the sequence safety functions will be *demanded* by all the sequence transient paths, for instance because the corresponding safeguard initiation signals or operator alarms are being activated. The delineation process may then be interpreted as valuing the probability of the demand one or zero for the set of all transient paths with the same sequence headers, all of them either as damage or success paths. Provided no damage path is included implicitly in any success sequence, (a fact difficult to prove when considering the grouping of initial faults, initial conditions and boundary conditions of the grouped transients in every single sequence) this approach is conservative, but it may be nonetheless unrealistic, leading for instance to a wrong perception of dominant

failure sequences whose frequency has been actually “inflated” due to the path grouping delineation process.

Stated in other way, the frequency calculation methods described in prior items are able to calculate the sequence frequency conditioned to the sequence being actually demanded by the decision making system, either the automatic protection system or the crew (indeed the result has units of frequency per demand). It is then necessary to multiply their results by the frequency of the demand. Traditional PSA techniques assume the probability of the demand either one or zero and this constitute the main objective of the sequence delineation process. This assumption is easy to prove right when the decision for interventions is automatic, and instantaneous execution of the orders issued can be defended. For other cases however, mainly manual actions taken after a non-negligible diagnostic time, more detailed consideration of the probability of the demand is in order, or some means ought to be provided to account for timing between the events of the sequence.

In summary , we can grossly say that:

Damage sequence frequency (year-1) =
*frequency of the set of ET/FT sequence headers (year-1/sequence demand)**
*probability of the demand **
fraction of sequence paths leading to violation of the safety limit.

and the last two terms are taken either zero or 1 in the traditional analysis, the first being extensively discussed in section --- earlier.

However, if these approximations are too conservative, yielding unacceptable frequency numbers, additional headers (provided they can be proved to be demanded) may be used to further discriminate the damage path groups that may have been mixed together with an excessive number of success paths. Or modifications to the header success and failure criteria may be attempted, the header success criteria becoming sequence dependent, as for instance available time considerations for human actions. Either way, it is necessary a detailed thermal-hydraulic analysis to show that the regrouping result is acceptable. This proof has the same purpose as the design safety accident analysis, but it may require additional ones. If there is no room for it, changes in the design as for instance modifications of header systems reliability or of the decision-making system (automatic or manual) are in order.

Therefore, we aim to obtain a table (see Table 3) with three columns:

- The first one would reproduce the results of damage exceedance frequency obtained in the classical PSA approach.
- The second one would provide the sequence demand probability (computed from a combination of the individual demand probabilities of each protection system intervening in the sequence), that corrects the PSA assumption that the exceedance frequency given is ‘per demand’, each individual protection system having a demand probability equal to 1.

- The third column would provide the fraction of paths within a sequence actually producing damage (depending on the possible combinations of activation and transition times), that corrects the PSA assumption that the whole sequence produces damage (fraction of paths producing damage equal to 1).

	Classical PSA exceedance frequency	Sequence demand probability	Fraction of the sequence contributing to damage	Corrected SDTPD value of the exceedance frequency
Sequence 1	A_1	B_1	C_1	$A_1 \cdot B_1 \cdot C_1$
…	…	…	…	…
Sequence s	A_s	B_s	C_s	$A_s \cdot B_s \cdot C_s$
TOTAL (i=1…s)	ΣA_i	-	-	$\Sigma A_i \cdot B_i \cdot C_i$

Table 3: Relation between the classical PSA exceedance frequency and SDTPD result, through multiplying factors expressing the demand probability and the fraction of the sequence contributing to damage.

Thus, the new value of the damage exceedance frequency, computed with the SDTPD approach, is a non-conservative value, because it corrects the PSA result with two factors between 0 and 1. In that way, any PSA analysis presented to the regulatory institution should give a value of the damage exceedance frequency higher than the new value of the SDTPD approach. In order to compute those factors, stimuli vector must be divided into three groups:

- Stimuli necessary to produce damage, $\{G_D\}$, whose contribution to the exceedance frequency would provide the factor of the second column (fraction of the sequence producing damage),
- Stimuli associated with the dynamic transitions of the sequence, $\{G_j\}$, whose contribution to the exceedance frequency would provide the factor of the third column (demand 'probability'),
- And a third group with the rest of the stimuli, whose contribution to the exceedance frequency would provide the result of the first column (exceedance frequency of the classic PSA approach).

The SDTPD equations of the ingoing density φ^n for a given sequence, characterized by a vector $\vec{j}_n$ of n dynamic transitions, yield to a sum of products of functions f^G (activation events) and h^G (dynamic events), integrated over all possible combinations of $\vec{\tau}$. Let's call 'cutset' every term of this sum. Obviously, there are f^G's and h^G's associated to each stimulus of the "damage stimuli" set $\{G_D\}$, and also to each stimulus in the "dynamic stimuli" set $\{G_j\}$. As the SDTPD is computed for a specific sequence $\vec{j}_n$, all the terms in the sum will contain the f^G's (their integrals over $\vec{\tau}$) corresponding to the activation of the dynamic stimuli, as well as the h^G's of their associated dynamic transitions (called in the sequel 'dynamic f^G's and h^G's'). Remark that, if some term of the sum does not contain some of the f^G's or the h^G's of the set $\{G_j\}$ associated to that sequence, it would indeed correspond to a different

sequence. On the other hand, some of the terms of the sum will contain all the f^G's of the damage stimuli set $\{G_D\}$ (called in the sequel 'damage f^G's') of a given damage D, meaning that all the stimuli necessary to produce damage D have been activated, and some others will not. Last ones could contain, though, the f^G's of a subset of the damage stimuli set $\left\{G_D^l\right\} \subset \left\{G_D\right\}$. Note that, if one of the dynamic transitions j of the sequence can be produced by several different stimuli, then the f^G's and the h^G's corresponding to that transition can be either of those of all the stimuli leading to it. Therefore, the set of dynamic stimuli can differ from one cutset k to another one, $\left\{G_j^k\right\}$. SDTPD ingoing density φ^n can be expressed as follows:

$$\varphi^n = \sum_k \left(\prod_{F \in \left\{G_j^k\right\}} f^F h^F \prod_{G \in \{G_D\}} f^G \cdot U_k \right) + \sum_l \left(\prod_{F \in \left\{G_j^l\right\}} f^F h^F \prod_{G \in \left\{G_D^l\right\} \subset \{G_D\}} f^G \cdot V_l \right) \tag{75}$$

where the first sum accounts for the cutsets going to damage and the second one for the cutsets going to a safe situation. Terms U_k and V_l contain the product of f^G's associated with the rest of (de)activation events. As we have seen, all the cutsets share the same sequence of dynamic transitions $\vec{j}_n$, but every cutset differs from each other in the sequence of (de)activation events (let us call it $\vec{J}_m$ for m (de)activations). On the other hand, cutsets resulted from the integration over $\vec{\tau}$ of all the possible paths. Thus, each of those cutsets corresponds to the grouping of paths that share a combined sequence of transitions $\left(\vec{j}_n, \vec{J}_m\right)$.

In order to compare this result of the SDTPD ingoing density with the exceedance frequency for a given damage D of the classical PSA, we have to integrate its product with a Boolean function indicating the presence of damage. Doing so, we eliminate all the non-damage cutsets, i.e., the second term of the right hand side of eq. (75):

$$\varphi^{exc}(D) = \sum_k \left(\prod_{F \in \left\{G_j^k\right\}} f^F h^F \prod_{G \in \{G_D\}} f^G \cdot U_k \right) \tag{76}$$

(again, we simplify notation by assuming that results of the integral are submerged into the coefficients).

The probability of a sequence s to be demanded is the combined probability that all the dynamic transitions of the sequence have been demanded, i.e., the product of the activation probabilities of all the stimuli inducing the dynamic transitions. Classical PSA approach assumes that the sequence has a probability of being demanded equal either to one or zero (in this case the sequence is not analyzed). As there may be several possible dynamic stimuli sets $\left\{G_j^k\right\}$, each with different combined probability in general, we define the **demand probability of sequence *s*** as the fraction:

$$B_s = \frac{\sum_k \left(\prod_{F \in \{G_j^k\}} f^F h^F \prod_{G \in \{G_D\}} f^G \cdot U_k \right)}{\sum_p \left(\prod_{F \in \{G_j^p\}} h^F \prod_{G \in \{G_D\}} f^G \cdot U_p \right)} \tag{77}$$

where the denominator can be interpret as the 'fully-demanded' sequence, closer to the PSA result for the exceedance frequency. Defined fraction B_s is the first correction factor (second column of the table above):

$$\varphi_s^{exc}(D) = B_s \cdot \sum_p \left(\prod_{F \in \{G_j^p\}} h^F \prod_{G \in \{G_D\}} f^G \cdot U_p \right) \tag{78}$$

Similarly, the probability of a sequence s to go to damage is the combined probability that all the stimuli necessary to produce damage have been activated, i.e., the product of the individual activation probabilities. Again, the classical PSA assumes a sequence completely going to damage or not, i.e., assuming that all the cutsets contain all the damage f^G's and that the combined probability is equal to one (damage sequence) or zero (success sequence). That would be equivalent to add the eliminated cutsets of the SDTPD ingoing density (second term of the right hand side in eq. (1)), and make the product of damage f^G's equal to one in all the cutsets. We define the fraction of a sequence s contributing to damage as the fraction:

$$C_s = \frac{\sum_p \left(\prod_{F \in \{G_j^p\}} h^F \prod_{G \in \{G_D\}} f^G \cdot U_p \right)}{\left[\sum_k \left(\prod_{F \in \{G_j^k\}} h^F \cdot U_k \right) + \sum_l \left(\prod_{F \in \{G_j^l\}} h^F \cdot V_l \right) \right]} \tag{79}$$

where the denominator can be interpret as the 'fully-demanded/fully-damaged' sequence, that reproduces the PSA result for the exceedance frequency. Defined fraction C_s is the second correction factor (third column of the table above):

$$\varphi_s^{exc}(D) = B_s \cdot C_s \cdot \left[\sum_k \left(\prod_{F \in \{G_j^k\}} h^F \cdot U_k \right) + \sum_l \left(\prod_{F \in \{G_j^l\}} h^F \cdot V_l \right) \right] \tag{80}$$

The first column of the table, i.e., the classical PSA result, is the 'fully-demanded/fully-damaged' sequence:

$$A_s = \sum_k \left(\prod_{F \in \{G_j^k\}} h^F \cdot U_k \right) + \sum_l \left(\prod_{F \in \{G_j^l\}} h^F \cdot V_l \right) \tag{81}$$

A more generalized definition of the three factors can be done based on the integration domains for the ingoing density φ^n. Denoting as D_I and D_i the integration time domains of the damage stimuli set and the dynamic stimuli set respectively, we can say:

$$\int \varphi^n \hat{D}_I \hat{D}_j = \int \varphi^n D_I D_j \cdot \frac{\int \varphi^n D_I \hat{D}_j}{\int \varphi^n D_I D_j} \cdot \frac{\int \varphi^n \hat{D}_I \hat{D}_j}{\int \varphi^n D_I \hat{D}_j} \tag{82}$$

damage — sequence fraction contributing to demand probability — classical PSA approach — SDTPD approach

where

$\hat{D}_I$ is the time integration domain where the damage stimuli are activated, and $\hat{D}_j$ is the time integration domain where the dynamic stimuli are activated.

8 Stimuli inventory: definition of the (de)activation and occurrence functions (*f* and *h*)

The most general definition of the stimuli (de)activation and event occurrence probability functions has to be made dependent on the continuous space of the state variables. In general, there will be two regions in that space: a region where the stimulus is deactivated (let us call it region 0) and another region, complementary to the first one, in which the stimulus is activated (called region 1), separated by a boundary (setpoint). If we assume at this point that only one variable x determines the state of a given stimulus G, then the continuous space will be the real line, or a finite interval on it, and the setpoint x_{sp} will be a point within that interval. If the variable x crosses the setpoint from region 0 to region 1 will activate the stimulus, and then there will be a function f^+ associated to that change. On the other hand, crossing the setpoint from region 1 to region 0 will deactivate the stimulus, and it will be characterized by a function f^-. All the time the variable x stays in region 1, i.e., the stimulus is activated, there is a probability h of the dynamic change associated to that stimulus being produced. This can be seen schematically in Figure (14):

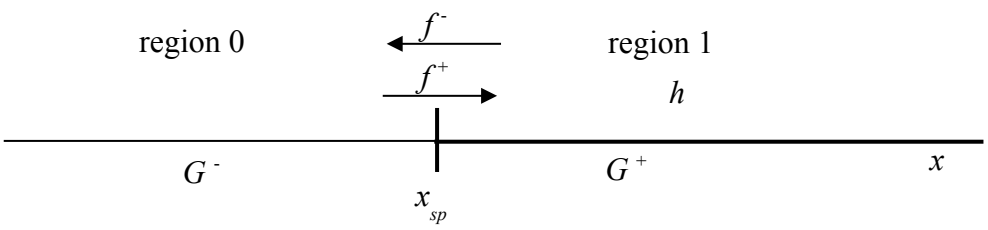


Figure 14: Single setpoint stimulus configuration.

meaning G^+ that the stimulus G is activated if x is in that region and G^- that it is deactivated. This kind of stimulus with 2 regions and a single setpoint is the most common in nuclear protections (release valve with a pressure setpoint, etc). Let us call this kind of stimulus ***single setpoint stimulus***.

When the function h depends on the variable x, we can further divide the activation region (region 1) into n subregions separated by additional setpoints, and each of them having different probability functions. This can be expressed schematically in the Figure 15:

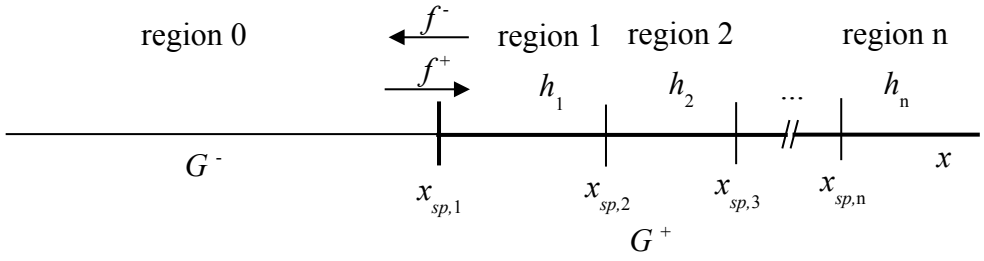


Figure 15: Region setpoint stimulus configuration.

This can be the case, for instance, of hydrogen combustion in PSA level 2: depending on the concentration of H_2 in the containment, there can be different probability for the hydrogen combustion. This kind of stimulus will be called ***region setpoint stimulus***.

To model stochastic phenomena, once the corresponding stimulus has been activated, the dynamic transition depends on a transition rate λ, indicating the probability per unit time of occurring the stochastic event. The delay pdf h is given in this case by the exponential equation:

$$h(t) = q_{dyn} e^{-\lambda t} \tag{83}$$

where q_{dyn} is the probability of occurring the event. This kind of stimulus can be denoted as ***λ-transition rate stimulus***.

Additionally, there are some cases in which the activation of a given stimulus is not triggered by the crossing of a setpoint in the state variables, but due to the activation of another stimulus. This kind of activation does not introduce any additional probability in the SDTPD theory, as is automatic and depends on the activation probability of another stimulus. There is in the SDTPD a Boolean matrix Ω that takes into account those associations among stimuli (de)activations, and acts on the stimuli vector J, changing the state of all the stimuli associated to the (de)activation of the 'driving' one (see chapter on the definition of the Ω matrices. This kind of stimulus will be called ***Ω-associated stimulus.***

There is another common case of stimuli in the nuclear safety analysis: when several stimuli can yield to the same dynamic event. This can also be seen as a single stimulus having different 'activation modes', i.e., depending on more than one variable of the state vector. Then the real line representing the continuous space of the stimulus associated variable x would become a N-dimensional space, where N is the number of activation modes being considered. Let's see the most simple case, in

which the stimulus depends on two variables and there is a single setpoint for each of them. Figure 16 shows the (de)activation regions for this kind of stimuli:

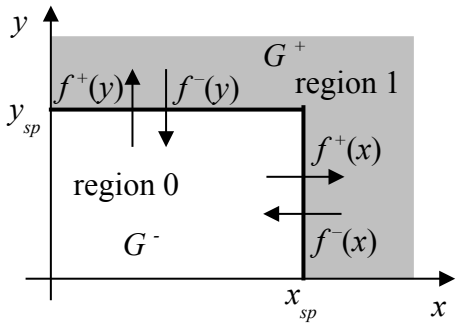


Figure 16: Region setpoint stimulus configuration.

This kind of stimuli can be defined as ***multiple-mode stimulus***, as it can be activated by different modes (state variables).

Table 4 presents the definition of the generic (de)activation and dynamic transition delay pdf's *f* and *h* for the stimuli inventory presented above.

Type of stimulus	Regions	Setpoints	Associated variable	Stimulus activation pdf f^+	Stimulus deactivation pdf f^-	Transition delay pdf h	Delay
Automatic setpoint stimulus	2	1	x_i	$q_+\delta\left(t-\tau_{sp}^+(x_i)\right)$	$q_-\delta\left(t-\tau_{sp}^-(x_i)\right)$	$q_{dyn}\delta(t)$	NO
Manual setpoint stimulus	2	1	x_i	$q_+\delta\left(t-\tau_{sp}^+(x_i)\right)$	$q_-\delta\left(t-\tau_{sp}^-(x_i)\right)$	$q_{dyn}h(t)$	YES
Region setpoint stimulus	n	n-1	x_i	$q_{+,2}\delta\left(t-\tau_{sp,2}^+(x_i)\right)+$ $+q_{+,3}\left(1-q_{+,2}\right)\delta\left(t-\tau_{sp,3}^+(x_i)\right)+$ $+q_{+,n}\prod_{k=2}^{n-1}\left(1-q_{+,k}\right)\delta\left(t-t_{AD}\right)$	$q_{-,1}\delta\left(t-\tau_{sp,1}^-(x_i)\right)$	$q_{dyn,2}h_2(t)$ $q_{dyn,3}h_3(t)$ ... $q_{dyn,n}h_n(t)$	YES
λ-transition rate stimulus	2	1	x_i	$q_+\delta\left(t-\tau_{sp}^+(x_i)\right)$	$q_-\delta\left(t-\tau_{sp}^-(x_i)\right)$	$q_{dyn}e^{-\lambda t}$	NO
Ω-associated stimulus	-	-	-	Ω^+	Ω^-	Ω^{dyn}	NO
Multiple mode stimulus	2	1	$x_1\, x_2 \ldots\, x_n$	$q_+\delta\left(t-\tau_{sp}^+(x_1)\right)+$ $+q_+\delta\left(t-\tau_{sp}^+(x_2)\right)+$ $+q_+\delta\left(t-\tau_{sp}^+(x_n)\right)$	$q_-\delta\left(t-\tau_{sp}^-(x_1)\right)+$ $+q_-\delta\left(t-\tau_{sp}^-(x_2)\right)+$ $+q_-\delta\left(t-\tau_{sp}^-(x_n)\right)$		YES

Table 4: Definition of the main characteristics of the stimuli inventory.

9 Benchmark exercise of containment failure by H_2 combustion

We propose to accomplish a benchmark exercise in order to test the behaviour of the SDTPD as a dynamic risk assessment methodology. The benchmark exercise proposed concerns containment failure risk assessment due to hydrogen combustion in case of water injection during in vessel core degradation for a French 900MWe PWR. This exercise is based on the results of two transitories computed by ASTEC in which there is no water injection, the first one without spray system activation and the second one with spray system activation. The description of the transitories is the following:

- There is a LOCA initiating event with a 3'' break size in a cold leg of RCS.
- Core uncovery starts at t_{cu} = 4080s (1h08min).
- Total core uncovery occurs at t_{tcu} = 5875s (1h38min).
- In the second transitory, the spray system starts at t_{spr} = 7000s (1h57min).
- Vessel rupture occurs at t_{vr} =14220s (3h57min).

The following example definition makes reference to "step 1" and "step 2" of the benchmark. Step 1 is the basic example. Step 2 contains some more details and extensions regarding stochastic events, but it is still a very simple model.

9.1 Benchmark exercise: specifications

This chapter presents the main assumptions proposed for the benchmark exercise. These assumptions have been proposed to avoid direct use of severe accident code and to allow an analytical assessment. Lack of precision in results due to these assumptions is not supposed to be quantified in the benchmark:

Assumption 1: before spray activation, there is no evolution of containment gas phase except for hydrogen. Values in Table 5 have been extracted from the ASTEC V0.4 calculation at 7000 s.

Total pressure (abs)	0.234 MPa
Average vol. Gas Temperature	108.9 °C
N_2 number of moles (mass)	1390372 (38910 kg)
O_2 number of moles (mass)	368384 (11788 kg)
Steam number of moles (mass)	1717196 (30909 kg)
Total number of moles	3475952

Table 5: State of the gas mixture in containment before spray system activation.

During the transient, before spray system activation, the number of moles of hydrogen and oxygen are supposed to change following assumptions 2, 3, 9, 10. The total number of moles of steam is supposed to be constant (thermal equilibrium).

The total pressure at time t, before spray system activation, is calculated by :

P(t) = P(7000s)*Nb_tot(t)/Nb_tot(7000s)

where Nb_tot is the number total of moles. P(7000s) = 0.234 MPa, NB_tot(7000S)=3475952.

Temperature of gas mixture stays constant before spray system activation (thermal equilibrium).

For step 2 of the exercise, the point values, given in table 1 and selected at 7000 s, are supposed to be uncertain and are distributed (uniform distribution) between the value given in Table 6 (these values have been extracted from ASTEC V0.4 calculation at 1400 s and 4300 s). N2 and O2 number of moles remain constant.

Total pressure	0.2 MPa	0.25 MPa
Average vol Gas Temperature	96.6 °C	110.4 °C
N_2 number of moles (mass)	1390372 (38910 kg)	1390372 (38910 kg)
O_2 number of moles (mass)	368384 (11788 kg)	368384 (11788 kg)
Steam number of moles (mass)	1383240 (24898 kg)	2034004 (36612 kg)

Table 6: State of the gas mixture in containment before spray system activation (min/max values).

Assumption 2: the hydrogen mass flow rate in the containment without water injection is given by the table 7 (extracted from ASTEC V0.4 results).

In Step 2 of the exercise, the uncertainty of the mass flow rate shall be represented by a factor between 0.5 and 1.5 (uniform distribution) to be multiplied to the flow rates below.

Time (s)	**H_2 flow rate without reflooding (kg/s) (Q_H2_without_water_injection)**	**H2 mass release (kg)**
4081	0	0
5340	0,00066	0,41
5660	0,028	5,00
5970	0,17	35,65
6110	0,36	74,18
6425	0,156	155,77
7005	0,04	212,28
7410	0,09	223,11
9180	0,034	340,13
11070	0	365,21

Table 7: Hydrogen flow rate towards containment without water injection.

Figures 17 and 18 allow comparison of table 6 (“data exercise”) with ASTEC V0.4 results.

The cumulative hydrogen release mass in containment can be calculated by the following way:

$$M\_H2(T_{N+1}) = M\_H2(T_N) + (Q\_H2(T_{N+1})+Q\_H2(T_N))/2*(T_{N+1}-T_N)$$

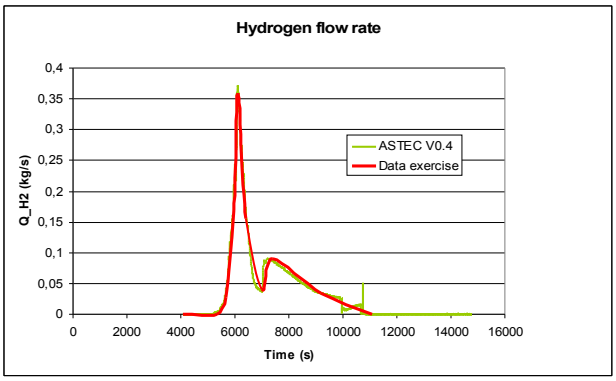


Figure 17: Hydrogen flow rate.

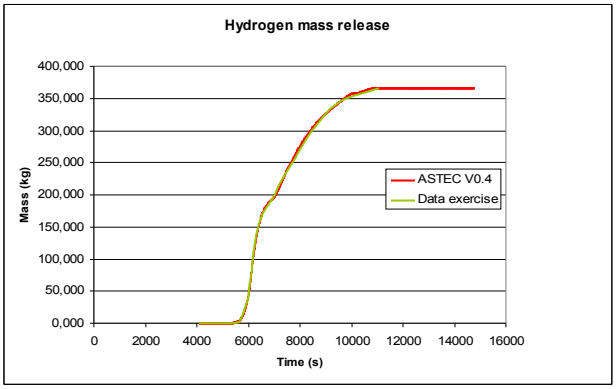


Figure 18: Hydrogen production (cumulated mass).

Assumption 3: in case of water injection, the water flow rate is supposed to be constant and equal to 27 tons/hour (7.5 kg/s). Between total core uncovery (at 5875s) and lower head failure (at 14 755s) all injected water is supposed to participate in the oxidation of Zr and steel ; the increase of the flow rate of hydrogen is supposed to be equal to 3 tons/hour (**0.833 kg/s**).

In step 2 of the exercise, the increase of hydrogen flow rate is to be assumed as follows:

- Water injection between total core uncovery (at 5875s) and 7000s produces 40% of the above rate (0.333 kg/s) with probability 0.3, 50% (0.416 kg/s) with probability 0.4 and 60% of the above rate (0.5 kg/s) with probability 0.3.
- Water injection between 7000s and formation of melting pool (9400s) is between 0.416 kg/s and 0.833 kg/s (uniform distribution)
- Water injection between 9400s and lower head failure produces 40% of the above rate (0.333 kg/s), with probability 0.3 50% (0.416 kg / s) with probability 0.4 and 60% of the above rate (0.5 kg/s) with probability 0.3.

Assumption 4: the maximum H_2 produced mass is equal to **950 kg** (oxidation of Zr and steel)

Assumption 5: the hydrogen flow rate in containment is calculated in the following way :

- before water injection: Q_H2(time) = Q_H2_without_water_injection(time)
- after water injection: Q_H2(time) = Q_H2_without_water_injection (time) + H2 flow rate given in assumption 3,
- if the mass of H2 release in containment is larger than 950 kg: Q_H2(time)=0.

If water injection occurs before the beginning of clad oxidation (4125 s), the situation is supposed to be saved: no hydrogen is produced and the vessel rupture is avoided.

Assumption 6: after the spray system activation, the containment steam mass (or number of moles) is changing and is given by the table 8.

In step 2 of the exercise, the times given in table 4 have to be modified as follows: the times to be added to T0 (i.e. 600s, 1500s, 2700s and 8000s) have to be multiplied by a common factor between 0.5 and 1.5 (uniform distribution), thereby simulating the influence of a more or less efficient spray. Use of this table will have to be consistent with assumption 1.

Time (s)	Steam mass (kg)	Steam number of moles
T_0 s (spray system activation)	30910	1717196
T_0+600	17433	968499
T_0+1500	7505	416979
T_0+2700	4181	232292
T_0+8000	2700	201399

Table 8: Evolution of steam mass in containment after spray system activation at T_0.

Figures 19 and 20 allow comparison with ASTEC V0.4 results.

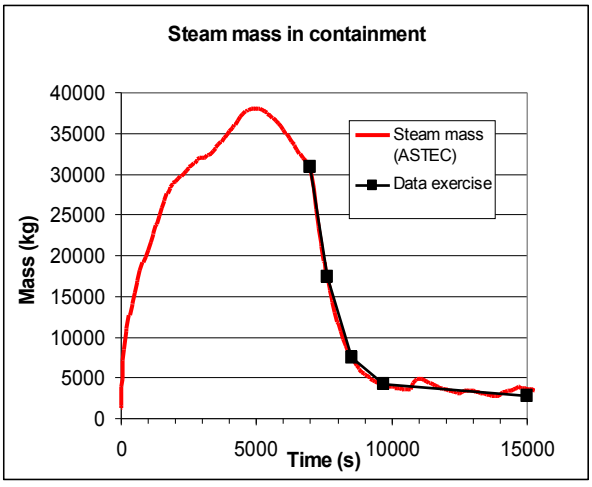


Figure 19: Evolution of steam mass in the containment after spray system activation.

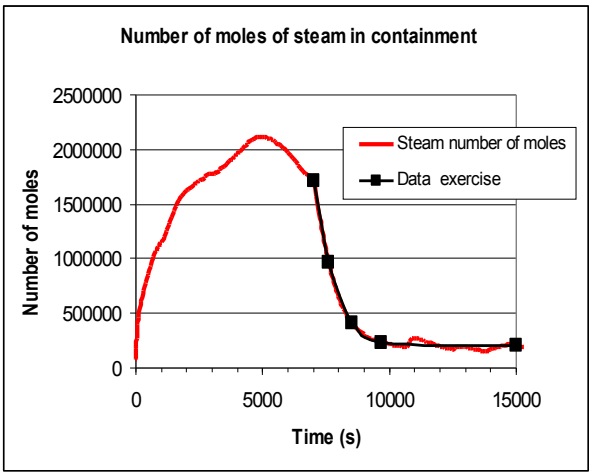


Figure 20: Evolution of steam number of moles in the containment after spray system activation.

Assumption 7: after the spray system activation, the average temperature of gas in the containment is given by the table 9. The impact of partial combustion on temperature is not taken into account.

For step 2 of the exercise see assumption 6.

Time (s)	**Average temperature of gas in containment (°C)**
T_0 s (spray system activation)	108.9
T_0+600	91
T_0+1500	73
T_0+2700	61
T_0+8000	55
T_0+13000	50

Table 9: Diminution of the average temperature of gas in the containment due to spray system activation at time T_0.

Assumption 8: after the spray system activation, the total pressure of gas in the containment is given by the table 10. To take into evolution of oxygen and hydrogen number of moles, the total number of moles of gas in containment can be used like in assumption 1 to correct the containment total pressure issued from ASTEC.

For step 2 of the exercise see note to assumption 6.

Time	Total pressure (MPa) in containment	Total number of moles (steam, H2,O2,N2) in ASTEC calculation
T_0 s (spray system activation)	0,234	3475952
T_0+600	0,178	2721994
T_0+1500	0,137	2161482
T_0+2700	0,121	1963907
T_0+8000	0,114	1893852

Table 10: Evolution of total pressure in containment after spray system activation

Assumption 9 : pressure peak in case of a total or a partial combustion

The pressure peak in case of a total or partial combustion has to be calculated by the function PAICC from ASTEC. This function will be provided by IRSN.

Input values of this function are :

Tg : Average temperature of gas in containment (°C)
P : total pressure in containment (bar)
[H20] : molar fraction of steam
[H2] : molar fraction of hydrogen
[O2] : molar fraction of oxygen
[N2] : molar fraction of nitrogen

Output value is PAICC.

The number of moles for steam, hydrogen, oxygen, nitrogen can be calculated following assumptions 1 to 6.

Total pressure in containment is calculated in function of total number of moles in containment like in assumption 1 (the steam number of moles depends on spray system activation, oxygen and hydrogen number of moles depend on combustion and recombination).

Molar fraction are deduced from the calculation of the number of moles.

Assumption 10 : mass flow rate of recombined hydrogen (and oxygen)

The mass flow rate (g/s) of hydrogen recombined by the PAR system is given by the following law :

Q_H2_rec = (K1* P + K2) [H2]
with K1 = 3. g/s/bar, K2=3.7 g/s, P= Pressure (bar),
[H2]= N_H2/N_tot*100,
N_tot = N_steam + N_N2 + N_02 + N_H2 (number of moles).

The mass flow rate (kg/s) for recombined oxygen is eight times the mass flow rate for hydrogen.

Impact of H2 and O2 and recombination on pressure in containment is taken into account like in assumption 1 (correction of pressure in function of total number of moles in containment).

In step 2 of the exercise K1 and K2 have an uncertainty band between 0.5 and 1.5 (uniform distribution) times the above values.

Assumption 11 : hydrogen distribution

Heterogeneity for hydrogen distribution is not taken into account (as discussed during the SARNET meeting of January 2006, these assumption is undoubtedly not relevant in case of high flow rate of hydrogen).

Assumption 12 : Combustion - Shapiro diagram

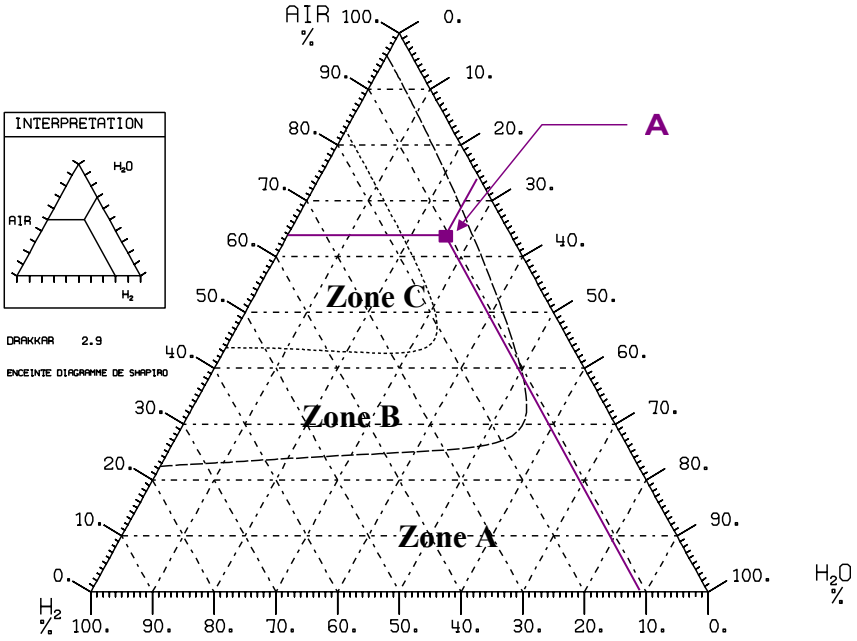


Figure 21: Shapiro diagram

The average containment gas mixture has to be placed in the Shapiro diagram.

Zone A: gas mixture is not flammable. No hydrogen combustion can occur
Zone B: gas mixture is flammable. Hydrogen combustion can occur
Zone C: not considered here.

The table 11 gives the limit for inflammability in terms of %H2 versus %H20.

[H20] (molar fraction in %)	[H2]infla (molar fraction %)
0	4
10	4.5
20	5.5
30	6.7
40	8.1
50	10.1

Table 11: Limit for inflammability

Assumption 13 – Ignition by recombiners

Recombiners are supposed to have an ignition capability. This ignition is due to the high temperature in recombiners and has been observed during experimental tests.

A combustion, ignited by recombiners, is supposed to occur in a short delay, if the following equation is satisfied (molar fraction in %):

if [H2] > $[H2]_{igni}$ with $[H2]_{igni}$= 5.2 + 0.0964*[H20].

Figure 22 allows comparison between limit of inflammability and limit of inflammation by recombiners. Mixture is flammable on the right side of the figure.

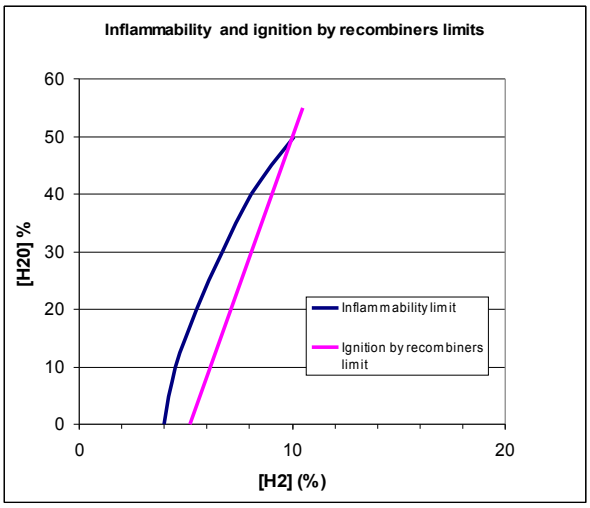


Figure 22: Comparison between limit of inflammability and limit of inflammation by recombiners

Assumption 14 – Delay before combustion

Delay before combustion is supposed to be as shorter as [H2] gets higher. To determine this delay, the following order of magnitude for delay are proposed :

- If [H2] < [H2]infla, no combustion can occur
- If [H2] = [H2]infla, the delay before the first (or after previous) combustion is distributed between 0 and 4 hours with a uniform probability distribution
- If [H2] >= [H2]igni, the delay before the first (or after previous) combustion is distributed between 0 and 0,333 hours (20 mn) with a uniform probability distribution
- If [H2]infla < [H2]< [H2]]igni, the delay before first (or after previous) combustion is distributed between 0 and Dtmax with an uniform probability distribution, where

Dtmax ([H2]) = (4{[H2]-[H2]igni}-0,333{[H2]-[H2]infla})/([H2]infla-[H2]igni)

Assumption 15 – Non total combustion

When a combustion occurs, it is supposed that it may be not total.

The fraction of burnt hydrogen in case of a combustion is distributed between 0,05 and 100 with a uniform probability distribution.

In step 2, the fraction of burnt hydrogen should depend on hydrogen concentration: fraction of burnt hydrogen is distributed between Fmin and 100 with uniform probability distribution. Fmin is provided by the following linear law :

$$Fmin = 0,05 + ([H2] - 4)*0,90/6$$

Assumption 16 – Water injection – description of the stochastic event

If water injection occurs before total core uncovery (5875 s), the situation is supposed to be saved : few hydrogen is produced and the vessel rupture is avoided. The probability of this situation is 0.5.

The probability that water injection is available between total core uncovery (5875s) and vessel rupture (14220s) is 0.5. The time when water injection starts is uniformly distributed between total core uncovery and vessel rupture.

In step 2 the probability of the availability of water injection follows a discrete distribution

0.3 with probability 20% ,
0.4 with probability 20% ,
0.5 with probability 30% ,
0.6 with probability 20% ,
0.7 with probability 10% .

Assumption 17 – Spray system activation – description of the stochastic event

The probability that the spray system can be activated after core uncovery (4080 s) and before vessel rupture is equal to 0.5. If the spray system can be activated, the time when spray system is activated is uniformly distributed between core uncovery (4080s) and vessel rupture.

In step 2 the probability of the availability of spray system follows a discrete distribution, for example

0.3 with probability 20% ,
0.4 with probability 20%,
0.5 with probability 30%,
0.6 with probability 20%,
0.7 with probability 10%.

Assumption 18 – Containment failure

To simplify the analysis of result, the containment will be first supposed to fail if overpressurization due to hydrogen combustion exceeds value Pmax_cont. The value 0.5 MPa will be retain as the reference case.

A more realistic assumption for containment could be considered in step 1. Table 12 provides containment failure probability in function of pressure peak.

Pressure peak (MPa)	Containment failure Probability
0.3	0
0.4	0.02
0.5	0.05
0.6	0.1
0.7	0.5
0.8	0.75
0.9	0.9
1	1

Table 12: Containment failure probability

In step 2, the containment failure probabilities in table 8 have to be multiplied by a common factor between 0.5 and 1.5 (uniform distribution) to take into account uncertainties (probability must no exceed 1).

Assumption 19 – Automatic spray system activation

No automatic spray system activation is considered.

A sensitivity calculation could be performed in step 2 : automatic spray system is supposed to be activated if containment pressure exceeds 0,24 MPa.

This chapter provides some limitations in the assumptions provided here for the simplicity of the exercise.

- Events like water injection, spray system start, ignition of the H2-H20-air mixture by recombiners should no be considered as independent,
- Evolution of containment gas composition and temperature should be considered with more details (steam condensation on walls, impact of water in sump, impact of combustion on gas temperature, impact of water injection on steam mass),
- Hydrogen distribution should not be considered as homogeneous in case of high hydrogen production,
- Uncertainties should have to be considered on ignition criteria by recombiners.

Obviously, some of these limitation could only be solved by the coupling between a severe accident code (with detailed models) and a dynamic reliability tool (step 3).

9.2 Physical description of the transient

The benchmark exercise introduces a stochastic character in the three main processes changing the dynamics: water injection, spray system and H_2 combustion. Recombiners act as a passive system being always available during the transient. The physical effects of those processes in the state variables are the following:

- Water injection: the only effect water injection is assumed to have is a constant increase in the hydrogen flow rate coming from the primary system (assumption 3).

- Spray system: it produces condensation in the containment atmosphere, i.e., a reduction in the steam number of moles given by table 4 (assumption 6). Additionally, it produces a decrease in temperature and total pressure given by tables 5 and 6 (assumptions 7 and 8). Total pressure change may be corrected proportionally to the total number of moles (assumption 1).

- Combustion: it reduces the number of moles of hydrogen according to the completeness coefficient (assumption 15), and increases the pressure with a peak computed with the function PAICC given by IRSN. It also reduces the number of moles of O_2 and increases the number of moles of steam, what is not clear in the specifications of the benchmark made by IRSN.

- Recombiners: they have the same effects that a combustion, i.e., reduction of number of moles of hydrogen and oxygen (assumption 10), except the peak of pressure. As they are catalytic recombiners, steam generated in the chemical reaction is not injected in the gaseous atmosphere, so there is not increase in the steam number of moles due to recombiners.

9.2.1 Boundary conditions

The following boundary conditions have to be applied:

- Hydrogen flow rate coming from the primary system (assumptions 2,3,4 and 5): is calculated in the following way:

  $J_H(t) = J_H^{no\_inj}(t)$ before water injection

  $J_H(t) = J_H^{no\_inj}(t) + J_H^{inj}(t)$ after water injection

  $J_H(t) = 0$ if the mass of H_2 released in the containment is greater than 950 Kg, or water injection occurs before the total core uncovery (5875s).

  where $J_H^{no\_inj}(t)$ is given by Table 3 of IRSN proposal and $J_H^{inj}(t)$ is given by assumption 3 of IRSN proposal (CSN proposal considers that only a fraction φ of injected water participates in the Zr and steel oxidation, so $J_H^{inj}(t)= 0.833\cdot\varphi$ Kg/s, being the rest of water directly injected into the containment in form of steam).

- Steam flow rate coming from the primary system (assumptions 2,3,4 and 5): IRSN does not consider any steam flow rate, even in the definition of the step 2 [H_2] flow rate, in which injection water is only partially used for oxidation of Zr and steel.

- Steam flow rate coming from the spray system (assumption 6): is given by the Table 4 (assumption 6) of the IRSN proposal. Before spray activation, *N_steam* is assumed to be constant (thermal equilibrium) (assumption 1). Thus, no increase of steam is assumed to occur with combustion.

9.3 Stochastic description of the transient

In this chapter we describe the three vectors involved in the SDTPD methodology (state, status and stimuli vectors) associated to this benchmark exercise.

9.3.1 State vector $\bar{x}$

Defines the variables involved in the transient.

- H_2 number of moles *N_H2*: it starts with a value given in table 1 (assumption 1); increases due to oxidation in the primary system according to table 3 (assumption 2) and due to water injection (assumption 3) until a maximum produced H_2 mass (assumption 4); and decreases due to recombiners (assumption 10) and due to combustion (assumption 15).

- O_2 number of moles *N_O2*: it is constant with a value given in table 1 (assumption 1) and only decreases due to recombiners (assumption 10) and combustion (not clear in the specifications).

- N_2 number of moles *N_N2*: it is constant during the entire transient and its value is given in table 1 (assumption 1).

- Steam number of moles *N_steam*: it is constant (thermal equilibrium) with a value given in table 1 (assumption 1) and only decreases due to the spray activation (assumption 6). Apparently, no increase of steam is assumed due to combustion.

- Total pressure in the containment *P*: its evolution is proportional to the total number of moles *N_tot* = *N_H2*+ *N_O2*+ *N_N2*+ *N_steam* (assumption 1). There are additional increases due to combustion (assumption 9) and a decrease associated to the spray activation (assumption 8).

- Gas mixture temperature *T*: it is constant (thermal equilibrium) with a value given in table 1 (assumption 1) and only decreases due to the spray activation (assumption 7).

9.3.2 Status vector $\bar{j}$

Describes the protections whose actuation may change the system configuration. Functions $h(t)$ are defined between t = 0s and $t = t_{vr}$. We distinguish between $h_i(t)$ for connection (i=initiate) of the system and $h_f(t)$ for disconnection (f=finish) of the system, which can be independent.

- Spray system θ_{spr}:
  - Function $h_{ispr}(t)$ is defined (assumption 17) equal to:

$$h_{ispr}(t) = \begin{cases} 0 & if \quad t \le t_{cu} \\ 4.93 \cdot 10^{-5} & if \quad t_{cu} < t \le t_{vr} \end{cases}$$

    where the second term comes from applying assumption 17 (h is uniformly distributed between t_{cu} and t_{vr} with probability 0.5).

$$\int_{t_{cu}}^{t_{vr}} h \cdot dt = 0.5 \qquad \rightarrow \qquad h = \frac{0.5}{(t_{vr} - t_{cu})}$$

  - Function $h_{fspr}(t)$ contemplates the disconnection of the system as a protection action itself or as a failure in operation. No disconnection nor failure of the spray system is assumed to happen in this benchmark:

$$h_{fspr}(t) = 0$$

- Water injection θ_{inj}:
  - Function $h_{iinj}(t)$ is defined (assumption 16) equal to:

$$h_{spr}(t) = \begin{cases} 8.51 \cdot 10^{-5} & if \quad t \le t_{tcu} \\ 5.99 \cdot 10^{-5} & if \quad t_{tcu} < t \le t_{vr} \end{cases}$$

    where the first term comes from applying assumption 16 (h is uniformly distributed between 0 and t_{tcu} with probability 0.5).

$$\int_{0}^{t_{tcu}} h \cdot dt = 0.5 \qquad \rightarrow \qquad h = \frac{0.5}{t_{tcu}}$$

    and the second term also comes from applying assumption 16 (h is uniformly distributed between t_{tcu} and t_{vr} with probability 0.5).

$$\int_{t_{tcu}}^{t_{vr}} h \cdot dt = 0.5 \qquad \rightarrow \qquad h = \frac{0.5}{(t_{vr} - t_{tcu})}$$

  - Function $h_{finj}(t)$: no disconnection nor failure of the spray system is assumed to happen in this benchmark:

$$h_{finj}(t) = 0$$

- Catalytic recombiners system θ_{rec}: it is considered as a passive system in the benchmark, so $\theta_{rec} = 1$ during the entire transient, and its influence on the dynamics requires $N\_H2 \neq 0$. However, we can consider t_{cu} as being the delay time for initiating recombiners (having the stimulus activated since t = 0) or as being the time setpoint for the stimulus activation with no delay in the occurrence of the event. In the first case, h would be reduced to a Dirac's delta:

$$h_{irec}(t) = \delta(t - t_{cu}) = \delta(t - 4080)$$

- Hydrogen combustion: as it is considered here a shock event, only causing sudden variations of some of the state variables, there is no necessity of Boolean variable to reflect its occurrence. However, it is characterized by a dynamic state that affects all the system, introducing new values to some of the state variables (numbers of moles of gases involved, total pressure, etc).
    - In the IRSN proposal there are defined two regions for initiating the combustion, the first due to the flammability conditions of the gases mixture, and the second one due to the ignition capability of the recombiners. A variable delay is defined for each region (assumption 14):

$$h_{icom}(t) = \begin{cases} \dfrac{1}{\Delta t_{\max}} & if \quad [H_2]_{flam} \le [H_2] \le [H_2]_{igni} \\ \dfrac{1}{1200} & if \quad [H_2] > [H_2]_{igni} \end{cases}$$

      where $\Delta t_{\max}$ is given by the following expression:

$$\Delta t_{\max}([H_2]) = \frac{\left(14400 \cdot ([H_2]_{igni} - [H_2]) + 1200 \cdot ([H_2] - [H_2]_{flam})\right)}{([H_2]_{igni} - [H_2]_{flam})}$$

    - As combustion is assumed to happen instantaneously, function $h_{fcom}(t)$ leading to partial combustions is substituted by a fraction of burnt hydrogen C, given by a uniform distribution between 0.05% an 100% (assumption 15). See also the "Finish combustion stimulus" below.

- Containment failure: as soon as the accident simulation ends when the containment failure is produced, there is no necessity of Boolean variable to reflect its occurrence.

9.3.3 Stimuli vector $\bar{J}$ (usually denoted as J)

Represents the fulfilment of the conditions that have to be triggered for the occurrence of a dynamic event:

- Initiate spray stimulus J_{ispr}:
    - It is activated at the beginning of the transient (automatic Ω activation associated to the initiating event).
    - The only way to deactivate it is the occurrence of the spray system dynamic event (automatic Ω deactivation associated to the dynamic event).

  Function $f_{ispr}(t)$ is thus defined as:

$$f_{ispr}(t) = (1 - J_{ispr})(1 - \theta_{inj})\delta(t) + J_{ispr}\delta(t - t_{spr})$$

  where the first term of the right hand side stands for the activation probability and the second term for the deactivation probability (no deactivation, other than the Ω one, can occur until the end of the transient).

- Finish spray stimulus J_{fasp}: once the spray system has been activated, it does not finish until the end of the transient.

$$f_{fspr}(t) = 0$$

- Initiate water injection J_{iinj}:
  - It is activated at the beginning of the transient (automatic Ω activation associated to the initiating event).
  - The only way to deactivate it is the occurrence of the water injection dynamic event (automatic Ω deactivation associated to the dynamic event).

  Function $f_{iinj}(t)$ is thus defined as:

$$f_{iinj}(t) = (1 - J_{iinj})(1 - \theta_{inj})\delta(t) + J_{iinj}\delta(t - t_{inj})$$

  where the first term of the right hand side stands for the activation probability and the second term for the deactivation probability.

- Finish water injection J_{finj}: once the water injection has started, it does not finish until the end of the transient.

$$f_{finj}(t) = 0$$

- Initiate catalytic recombiners stimulus J_{irec}:
  - It is activated at the beginning of the transient (automatic Ω activation associated to the initiating event).
  - The only way to deactivate it is the occurrence of the catalytic recombiners dynamic event (automatic Ω deactivation associated to the dynamic event).

  Function $f_{irec}(t)$ is thus defined as:

$$f_{irec}(t) = (1 - J_{irec})(1 - \theta_{rec})\delta(t) + J_{irec}\delta(t - t_{rec})$$

  where the first term of the right hand side stands for the activation probability and the second term for the deactivation probability.

- Finish catalytic recombiners stimulus J_{frec}: once the catalytic recombiners have been activated, they do not stop until the end of the transient.

$$f_{frec}(t) = 0$$

- Initiate combustion stimulus J_{icom}:
  - The activation condition is a setpoint with $[H_2] > [H_2]_{flam}$, where $[H_2]_{flam}$ is a function of $[H_2O]$.
  - The deactivation condition is the symmetric of the activation one, i.e., a setpoint with $[H_2] < [H_2]_{flam}$. This deactivation can occur due, for instance, to the hydrogen reduction caused by the catalytic recombiners.

  Function $f_{icom}(t)$ is thus defined as:

$$f_{icom}(t) = (1 - J_{com})\delta(t - t([H_2] > [H_2]_{flam})) + J_{com}\delta(t - t([H_2] < [H_2]_{flam}))$$

  where the first term of the right hand side stands for the activation probability and the second term for the deactivation probability.

- Finish combustion stimulus J_{fcom}: initially, combustions are supposed to be instantaneous, so the activation of this stimulus (and actually the occurrence of its associated dynamic event "finish combustion") would happen simultaneously with the beginning of the combustion. However, the effect of the real combustion time leading to partial combustions is substituted in this benchmark by a factor of combustion "completeness" C, that could be seen as the limit of the burnt H_2 fraction when the combustion time goes to zero.
  Function $f_{fcom}(t)$ is thus defined as:
  $$f_{fcom}(t) = (1 - J_{com})\delta(t - t_{com}) + J_{com}\delta(t - t_{com}) = \delta(t - t_{com})$$

- Rupture stimulus J_{rup}:
  - The activation condition is a setpoint p>0.5MPa, initially taken as a reference case (further refinement is proposed in assumption 18 of IRSN proposal)

  Function $f_{rup}(t)$ is thus defined as:
  $$f_{rup}(t) = (1 - J_{rup})\delta(t - t(P > P_{\lim}))$$

9.3.4 Dynamic states

According to the status vector $\bar{j}$, the following dynamic states can exist:

Dynamic state	Spray system	Water injection	Cat. recombiners
0	Off, θ_{asp}=0	Off, θ_{val}=0	On, θ_{rec}=1
1	Off, θ_{asp}=0	On, θ_{val}=1	On, θ_{rec}=1
2	On, θ_{asp}=1	Off, θ_{val}=0	On, θ_{rec}=1
3	On, θ_{asp}=1	On, θ_{val}=1	On, θ_{rec}=1
4	Combustion		
5	Rupture		

Table 13: Dynamic states of the system in the benchmark exercise.

9.3.5 Ω matrices

The Ω matrices are those which define stimuli (de)activations associated to another (de)activation or dynamic events, produced by 'father' or 'driving' stimuli. In that sense, there can be three different types of Ω-matrices: activation matrices, deactivation matrices and dynamic matrices. For this benchmark, the Ω-matrices are defined as follows:

Activation Ω-matrix

	Init. Spray	Init. Inject.	Init. Rec.	Combustion	Rupture
Init. Spray	1	0	0	0	0
Init. Inject.	0	1	0	0	0
Init. Rec.	0	0	1	0	0
Combustion	0	0	0	1	0
Rupture	0	0	0	0	1

Deactivation Ω-matrix

	Init. Spray	Init. Inject.	Init. Rec.	Combustion	Rupture
Init. Spray	-1	0	0	0	0
Init. Inject.	0	-1	0	0	0
Init. Rec.	0	0	-1	0	0
Combustion	0	0	0	-1	0
Rupture	0	0	0	0	-1

Dynamic Ω-matrix

	LOCA	Init. Spray	Init. Inject.	Init. Rec.	Combustion	Rupture
LOCA	0	1	1	1	0	0
Init. Spray	0	-1	0	0	0	0
Init. Inject.	0	0	-1	0	0	0
Init. Rec.	0	0	0	-1	0	0
Combustion	0	0	0	0	-1	0
Rupture	0	0	0	0	0	-1

9.3.6 Protection variables and damage variables

From all the state variables defined in the previous chapter, some of them or a combination of them determines the actuation of the protections along the accident, whereas some others lead to the activation of the damage stimuli, i.e., those stimuli whose activation is necessary to produce damage. Identifying these two sets of variables is a key part of the analysis, in order to be able to follow their evolution for an optimum transient analysis. Both sets of variables can have common elements.

- Damage variables: we first have to identify the damage stimuli subset. In that sense, the damage stimulus in this benchmark is the containment rupture stimulus J_{rup}, whose associated variable is the total pressure P.

  There are two dynamic processes increasing the pressure: the water injection event (by increase of the number of moles of H_2) and the combustion event. The first one is not capable by itself of producing damage, as the increase of pressure produced by the total available hydrogen (950kg) does not reach the pressure setpoint for containment failure. The second one, instead, is the only dynamic event capable of producing damage, through the pressure peaks caused by each combustion event. Thus, the initiate combustion stimulus J_{icom} is a stimulus necessary to produce damage and belongs to the damage stimuli subset. The variable controlling this stimulus is the flammability region, a function of $[H_2]$ and $[H_2O]$, in which the decrease of $[H_2O]$ also decreases the setpoint $[H_2]_{flam}$, leading to higher probability of combustion.

  Therefore, the damage stimuli subset is $\{J_{rup}, J_{icom}\}$ and the damage variables are P (increase), $[H_2]$ (increase) and $[H_2O]$ (decrease).

- Protection variables: protection actions are in this benchmark the water injection system activation, the spray system activation and the catalytic

recombiners system activation. Activation of the corresponding stimuli has no dependence on the state variables, as the three stimuli are activated since the beginning of the transient.

Therefore, there are no protection variables in this exercise.

10 Conclusions

Correct definition and determination of safety margins has become a key issue within the licensing and regulatory nuclear institutions. To compute safety margins, the most convenient figure of merit is the exceedance frequency of a given damage D_p. A consistent and robust methodology to accomplish the estimation of the exceedance frequency is therefore necessary. The Stimulus-Driven Theory of Probabilistic Dynamics (SDTPD) provides the appropriate mathematical framework to model the exceedance frequency coupled to the dynamic evolution of the accident transient and all its state variables, through the incorporation of the "stimulus" concept to reproduce the human-driven actions and the stochastic phenomena involved. We have presented the methodology and developed some detailed aspects leading to its numerical implementation. Nevertheless, there are still some theoretical steps to be done to accomplish this task. A benchmark exercise has also been proposed as future work to validate the methodology against the classical PSA approach and to point out the advantages that it provides.

REFERENCES

1. Akers, B. Binary Decision Diagrams. *IEEE Transactions on Computers*, 27(6):509–516, 1978.
2. Andersen H. R. *An Introduction to Binary Decision Diagrams*. `http://www.itu.dk/people/hra/notes-index.html`, 1997.
3. Bley D., Kaplan S., Johnson D., 1992. The strengths and limitations of PSA: Where we stand. *Rel. Eng. Syst. Safety* 38, pp. 3-26.
4. Bryant, R. E. Graph based algorithms for boolean function manipulation. *IEEE Transactions on Computers*, 35(8):677–691, 1986.
5. Devooght J., Smidts C., 1992a. Probabilistic reactor dynamics. I. The theory of continuous event trees. *Nucl. Sci. & Eng.* , pp. 229-240.
6. Devooght J., Smidts C., 1992b. Probabilistic reactor dynamics. III. A framework for time-dependent interaction between operator and reactor during a transient involving human error. *Nucl. Sci. & Eng.*, pp. 101-113.
7. Devooght J., Smidts C., 1996. Probabilistic dynamics as a tool for dynamic PSA. *Rel. Eng. Syst. Safety*, pp. 185-196.
8. Izquierdo, J.M. et al., Automatic generation of dynamic event trees: a tool for integrated safety assessment (ISA). In *NATO ARW on Reliability and Safety Assessment*, 24-28 August 1992, Kusadasi, Turkey. Springer Verlag, Berlin, 1994.
9. Izquierdo, J.M., Labeau, P. E. Modeling PSA problems – III: summary and application of the SDTPD. Draft.
10. Izquierdo J.M., Melendez E., Devooght J., 1996. Relationship between probabilistic dynamics and event trees. *Rel. Eng. Syst. Safety*, pp. 197-209.

11. Labeau, P.E., Izquierdo, J.M., (2004) The stimulus driven theory of probabilistic dynamics as a Framework for Probabilistic Safety Assessment, in Spitzer, C. Schmocker, U and Dang, V.H. eds, Probabilistic Safety Assessment and Management, proceedings of the PSAM-7/ESREL-04 Conference, Springer, Berlin, Germany.
12. Labeau, P. E., Izquierdo, J.M., 1995a. Modeling PSA problems – I: the Stimulus-Driven Theory of Probabilistic Dynamics. *Nucl. Sci. & Eng.* 150, pp. 115-139.
13. Labeau, P. E., Izquierdo, J.M., 1995b. Modeling PSA problems – II: a cell-to-cell transport theory approach. *Nucl. Sci. & Eng.* 150, pp. 140-154.
14. Rauzy, A. A brief introduction to Binary Decision Diagrams. *Journal Européen des Systèmes Automatisés*, 30(8):1033–1050, 1996.
15. Siu N., 1994. Risk assessment for dynamic systems: An overview. *Rel. Eng. Syst. Safety* , pp. 43-73.