The stimulus-driven theory of probabilistic dynamics as a framework for probabilistic safety assessment

J.M. IZQUIERDO
Consejo de Seguridad Nuclear
Justo Dorado 11, E - 28040 Madrid
jmir@csn.es
Fax: +34-913460496

P.E. LABEAU *
Université Libre de Bruxelles (CP165/84)
Av. F.D. Roosevelt 50, B - 1050 Brussels
pelabeau@ulb.ac.be
Fax: +32-2-6504534

Abstract

(ID: 0414)

The current version of the Theory of Probabilistic Dynamics (TPD) falls short in modeling essential aspects of PSAs, because automatic or manual actions that induce safety oriented events curbing undesired time evolutions, are always "stimulated" by particular features of the situation. Typical stimulus examples are initiation safeguards setpoints or control room alarms, but many others, as the influence of organizations in the operator interventions are also to be accounted for. To incorporate the concept of stimulus covering all those circumstances into the TPD was the purpose of two recent papers that describe the resultant Stimulus-Driven Theory of Probabilistic Dynamics (SDTPD). However, the theory is still general and does not introduce the familiar concept of sequences. This summary paper shows how sequences may also be incorporated into SDTPD in order to better understand PSA. A set of equations derived from this new extension is able to provide exceedance frequency and sequence probability under the same assumptions as those of current PSA methods. SDTPD is also presented in a more refined version with a symmetric treatment of stimulus activation and disactivation events, and allows the probabilities of the next event to depend on the state of all stimulus.

1 Introduction

The PSA methodology is widely used in the nuclear industry as a systematic process to integrate partial elements into a coherent risk analysis. One of its challenges is the consistent treatment of the dynamics of the evolution of accidents and transients (accident analysis), and its interface with systems features that are critical to the outcome of accidents (system reliability). A rigorous theory supporting this consistency is still in need, as pointed out in many places (Bley et al., 1992, Siu, 1994). Promising candidates include the Theory of Probabilistic Dynamics(TPD) (Devooght and Smidts, 1992, Smidts and Devooght, 1992, Devooght and Smidts, 1994). However, its current version falls short in modeling essential aspects of PSAs, because in reality automatic or manual actions that induce safety oriented events curbing undesired time evolutions , are always "stimulated" by particular features of the situation.

*Research Associate, National Fund for Scientific Research (Belgium), corresponding author

Moreover, stochastic delays between stimulus activation (activation events) and the dynamic event occurrence may generate competing situations influencing the time and nature of the next dynamic event. Both effects are not modeled within TPD, but are implicit in many assumptions underlying the PSA method . In two recent papers (Labeau and Izquierdo, 2003 I, 2003 II), heretofore ref.L, we aimed at solving these drawbacks through appropriate extensions that force to abandon the semi-Markov assumption, the probability of the next event being now a function of the times of activation of stimuli.

We will focus in this summary paper in showing the adequacy of SDTPD to understand the PSA methodology, by introducing the concept of paths and sequences and deriving a set of associated PSA evolution equations.

2 Summary of the stimulus driven TPD

2.1 Modeling the plant states

SDTPD includes an additional extension of the state space: stimulus activation states are considered through a stimulus label indicating the activated ($I_G = +$) or disactivated ($I_G = -$) state of stimulus G. The notation I will be reserved to label these state configurations when considering all stimuli together. A so-called stimulus is either an order for action (in many cases given by an electronic device or corresponding to an operator diagnosis), or the fulfillment of conditions triggering a stochastic phenomenon. Yet it can take many different forms, such as the crossing of a setpoint or the entry in a region of the process variables space. In general, the term stimulus covers any situation which potentially causes, after a given time delay, an event to occur and subsequently a branching to take place.

Fig 1 shows the SDTPD modeling of events. $f_i^F(t, \bar{u})$ is the probability per unit time of activating stimulus F a time t after entering dynamics i at $\bar{u}$ and $h_{ij}^F(t, \bar{u})$ that of a delay t to generate dynamic event ij after activating stimulus F at $\bar{u}$. The total system state in the course of a transient is thus defined by the couple (i,I), which accounts at the same time for the current dynamics, i, in which the system evolves, and for the current status of the different activations. The system evolution therefore appears as a piecewise-deterministic stochastic process between these combined states.

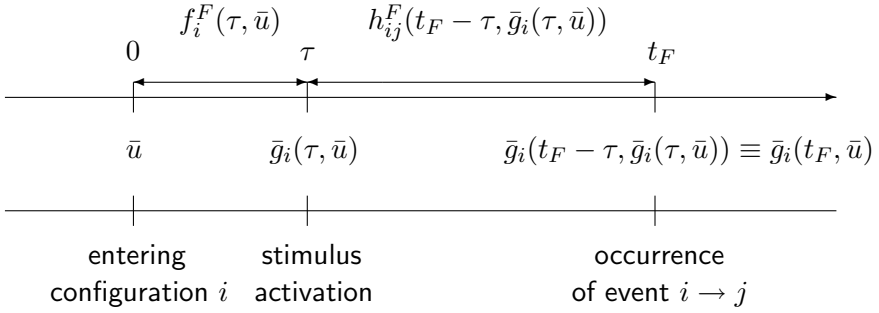

Figure 1: Two-phase occurrence of the F-induced event

2.2 Modeling the probability of the next event

Let $\bar{x}$ be the vector of process variables describing the dynamic behaviour of the system. We denote by i the group of system configurations in which the dynamic evolution is given by the equivalent explicit form

$$\bar{x}(t) = \bar{g}_i(t, \bar{x}_o),\ \bar{x}_o = \bar{g}_i(o, \bar{x}_o) \tag{1}$$

We define the ingoing density $\varphi(\bar{x}, (i, I), t)$ such that $\varphi(\bar{x}, (i, I), t)dx$ is the probability per unit time of entering state i,I at time t with $\bar{x}$ between $\bar{x}$ and $\bar{x} + d\bar{x}$. When integrated over the whole $\bar{x}$ space, this density becomes the familiar PSA frequency.

The states of the corresponding non-Markov process cannot be characterized only by the couple (i, I). Indeed, the time of the last modification of the activation state of each individual stimulus must be kept in memory, as well as the time of the last change of dynamics. Let $\vec{\tau}_{(i,I)}$ denote the vector collecting all these instants. This vector has thus to be associated with (i, I) to fully describe this state.We denote by τ_j the entry time in dynamics j, and by τ_G^J the time of the last (dis)activation of stimulus G, in the global activation state J. τ denotes the time of the last entry in a combined state, before entering (i, I).

In semiMarkov TPD, $q_{ji}^{JI}(t - \tau, \bar{u})dt$ is the probability of the transition $(j, J) \to (i, I)$, a time between t and $t + dt$ after entering state (j, J) at point $(\tau, \bar{u})$. Since we are no longer in the semi-Markov frame, q_{ji}^{JI} depends on both t and τ, and not on the time difference $t - \tau$. This probability per unit time must also give allowance to vector $\vec{\tau}_{(j,J)}$, both before and after the next event; its extension will be denoted by Q.

2.2.1 Dependence in stimulus activations

Let $\tilde{Q}_j^{J,G}(t; \tau, \bar{u}, \vec{\tau}_{(j,J)})dt$ be the probability of the (dis)activation of stimulus G in $[t, t + dt]$ in state (j, J) entered at $\vec{\tau}_{(j,J)}$, the last event having occurred at $(\tau, \bar{u})$. We also introduce the Boolean function $\Omega_j^G(J \to I)$, which embodies the effect of the (dis)activation of stimulus G in dynamics j on the global activation state, making it change from J to I. This Boolean function thus defines which stimuli can lead to the transition $J \to I$, and are therefore to be considered. Let $\mathcal{A}_G(j, J)(\ni G)$ be the set of stimuli whose activation state was modified in this transition. Similarly let $\hat{Q}_{ji}, \Omega_{ji}$, and the set $\{G_{ji}\}$ be their counterparts for the corresponding dynamic events. Then, we can structure Q as follows :

$$\begin{aligned} Q_{ji}^{JI}(t, \vec{\tau}_{(i,I)}; \tau, \bar{u}, \vec{\tau}_{(j,J)}) \;=\; & \delta_{ji}\delta(\tau_j - \tau_i) \sum_G \tilde{Q}_j^{J,G}(t; \tau, \bar{u}, \vec{\tau}_{(j,J)}).\Omega_j^G(J \to I) \\ & \times \prod_{F \in \mathcal{A}_G(j,J)} \delta(t - \tau_F^I). \prod_{H \notin \mathcal{A}_G(j,J)} \delta(\tau_H^J - \tau_H^I) \\ & + (1 - \delta_{ji})\delta(t - \tau_i)\hat{Q}_{ji}^J(t; \tau, \bar{u}, \vec{\tau}_{(j,J)}).\Omega_{ji}(J \to I) \prod_{G \in \{G_{ji}\}} \delta(t - \tau_G^I) \prod_{H \notin \{G_{ji}\}} \delta(\tau_H^J - \tau_H^I) \end{aligned} \tag{2}$$

The interpretation of this splitting is straightforward: if the next event is an activation event, the entry time in the current dynamics is unaffected, and so are the activation times of all the stimuli but those which have been (dis)activated; if, on the other hand, the next event is a dynamic event, all stimuli disactivated as a result of the change of dynamics have their new activation times equal to t, while the activation times of the unaffected stimuli are unchanged.

2.3 Evolution of the ingoing density

Let $\varphi(\bar{x},(i,I),t,\vec{\tau}_{(i,I)})$ be the ingoing density in state (i,I) entered at time $\vec{\tau}_{(i,I)}$. $\varphi(\bar{x},(i,I),t,\vec{\tau}_{(i,I)})$ must then vanish for all times t, except when t corresponds to the maximum of the components of $\vec{\tau}_{(i,I)}$. This condition has been included in the probabilistic kernel Q_{ji}^{JI} given above. Its evolution equation then becomes:

$$\begin{aligned}\varphi(\bar{x},(i,I),t,\vec{\tau}_{(i,I)}) &= \sum_{(j,J)\neq(i,I)} \int_o^t d\tau \int d\bar{u} \int_o^\tau d\tau_j \left(\prod_G \int_o^\tau d\tau_G^J\right) \delta(\bar{x}-\bar{g}_j(t-\tau,\bar{u})) \quad (3)\\ &\times \left[\pi(\bar{u},(j,J),\tau)\delta(\tau)\delta_{J,I_o}\delta(\vec{\tau}_{(j,J)}) + \varphi(\bar{u},(j,J),\tau,\vec{\tau}_{(j,J)})\right] Q_{ji}^{JI}(t,\vec{\tau}_{(i,I)};\tau,\bar{u},\vec{\tau}_{(j,J)})\end{aligned}$$

that can be easily understood: the plant enters configuration i,I at time t with process variables $\bar{x}$, either if it has been in configuration j,J from the beginning of the transient, following dynamics $\bar{g}_j(t-\tau,\bar{u})$ during a time $t-\tau$, or if the last transition to configuration j,J took place at time $\tau<t$. In the first case we set $\tau=0$, and $\pi(\bar{u},(j,J),\tau)$ is the probability of starting from initial conditions $\bar{u},(j,J)$.

2.3.1 Semi Markov and Markov TPD

It has been shown in ref.L that in the particular case $\Omega_{ji}(J\to I)=\delta_{II_0}$, $\Omega_j^G(J\to I)=\delta_{II_0}$ that is, all activated stimuli become disactivated at any event , the ingoing density, when integrated in variables $\vec{\tau}_{(i,I)}$, satisfies the standard semiMarkovian TPD equations when using as the probability of the next event

$$\begin{aligned}q_{ij}(t;\bar{u}) \equiv \sum_F q_{ij}^F(t;\bar{u}) &= \sum_F \int_o^t f_i^F(\tau;\bar{u}) h_{ij}^F(t-\tau;\bar{g}_i(\tau,\bar{u}))\, d\tau\\ &\cdot \prod_{G\neq F}\left[1-\int_o^t dt' \int_o^{t'} d\tau f_i^G(\tau;\bar{u}) h_i^G(t'-\tau;\bar{g}_i(\tau,\bar{u}))\right] \quad (4)\end{aligned}$$

Of particular interest is the Markov case in which components F may fail with transition rates $p^F(i\to j|\bar{x})$. We can interpret this situation as stimulus induced events with

$f_i^F(t;\bar{u})=\lambda_i^F(\bar{g}_i(t,\bar{u}))e^{-\int_o^t \lambda_i^F(\bar{g}_i(s,\bar{u}))ds}$, i.e. the pdf of leaving i after surviving other component F events in configuration i a time t after entering it at point $\bar{u}$. Also

$h_{ij}^F(t;\bar{u}) \equiv p^F(i\to j|\bar{u})/\lambda_i^F(\bar{u})\delta(t)$, i.e. the pdf of transitioning from i into state j with no delay.

With this interpretation, eq.(3) reduces to the standard Markovian TPD. This shows the consistency of SDTPD and the strong and unrealistic assumptions implied by TPD concerning stimulus activation.

2.4 Operator actions and uncertain phenomena

In the general case, ref.L gives the relations between $\hat{Q},\tilde{Q}$ and the f, h pdf for each event type. In order to provide explicit expressions to represent operator stimuli and uncertain phenomena, let us assume that experiments on phenomenon F provide activation probabilities $q_{M_j}^F$ in regions $M_j, j=1\ldots n$, partitioning the phase space. Or consider an operator having a probability $q_{M_j}^F$

to diagnose a problem F when the system lies within region M_j, the delay corresponding to his/her time to action after diagnosis. How can the pdf of the activation time in dynamics i be built in such cases? Let $\tau_{ij}^F(\bar{u})$ be the time required, while evolving in dynamics i from $\bar{u}$, to reach the border of the jth region M_j visited by the system trajectory in the process variables space, given these regions are ranked in the order they are entered along the process variables evolution in dynamics i. If we assume stimulus F is instantaneously activated when entering a region, we can write, with t_{AD} the accident duration or mission time:

$$\begin{aligned} f_i^F(t;\bar{u}) &= q_{M_1}^F \delta(t-\tau_{i1}^F(\bar{u})) + (1-q_{M_1}^F) q_{M_2}^F \delta(t-\tau_{i2}^F(\bar{u})) \\ &\quad + (1-q_{M_1}^F)(1-q_{M_2}^F) q_{M_3}^F \delta(t-\tau_{i3}^F(\bar{u})) + \dots \\ &\quad \dots + \prod_{j=1}^{n} (1-q_{M_j}^F).\delta(t-t_{AD}) \end{aligned} \tag{5}$$

with $\tau_{i,j+1}^F(\bar{u}) > \tau_{ij}^F(\bar{u}), \forall j$. This expression is a generalization of simpler ones and it may be shown to include most situations of interest, as those describing setpoint stimulus. Similar relations may be used for the delays, although they seldom require this level of complexity.

3 Application to classical PSA

3.0.1 Paths and sequences

Once the general framework has been established, we are in a position to show how the classical fault tree/event tree (FT/ET) analysis is derived as a particular case. We will assume in the following that:

- the system starts at a steady point state $\bar{u}_0, j_0, J_0$ with given probability there. A random instantaneous dynamic initiating event with a known frequency triggers the time evolution.
- process variable $\bar{x}$ can be reached from the initial point state only after one sequence of dynamic events through a compound path defined by

$$\overline{x}_n = \overline{u}_{\vec{j}_n}(t, \vec{\tau}_{j_n}) \equiv \overline{g}_{j_n}(t-\tau_{j_{n-1}}, \hat{\overline{u}}_n) \quad t \geq \tau_{j_{n-1}} \quad \overline{u}_{\vec{j}_n}(\tau_{j_{n-1}}, \vec{\tau}_{j_n}) \equiv \hat{\overline{u}}_n = \overline{u}_{\vec{j}_{n-1}}(\tau_{j_n}, \vec{\tau}_{j_{n-1}}) \tag{6}$$

Each of the dynamic time variables $\vec{\tau}_{j_n} = (\tau_{j_1}, \tau_{j_2}, ...\tau_{j_{n-1}}, \tau_{j_n})$ coincides with some of the dynamic event time variables τ_i, but ordered in increasing time, the evolution from the initial state determining its sequence of appearence.

Under the given assumptions, once the possible dynamics and initial point state are defined, the paths possible may be determined including its timing. We will call a sequence the set of paths $\left\{(\vec{j}, J), \vec{\tau}_{\vec{j},J}\right\}$ with the same $(\vec{j}, J)$, but differing in the timing.

This consideration leads to replace the complicated multidimensional domain of integration over $\bar{u}$ in eq.(3) by the aggregation of all possible paths, the set expanding as a tree as time goes. The price to pay for the sequence and paths assumptions is that there are many paths possible within a sequence. Each path represents a deterministic transient that may be computer simulated with available simulation technology. However, identifying the relevant stimulus and the paths within a sequence that activate events, is a complex and key factor in the process

of sequence delineation. The relevant paths constitute a sequence envelop that should also take into account the bounding of the damage they may generate (as for instance design basis envelops)

3.1 Evolution equations for the ingoing density: the PSA equations

Because we assume that at most one path n links $\bar{u}_0$ with a given $\bar{x}$, we can write, with n the number of dynamic events occurred prior to time t,

$$\varphi(\bar{x},(i,I),t,\vec{\tau}_{(i,I)}) = \sum_{n=1}^{\infty}(\varphi^n_{ET}(\bar{x}_n,(i_n,I),t,\vec{\tau}_{(i_n,I)})\delta(\bar{x}-\bar{x}_n)\delta(t-\max_G \tau^I_G)\theta(t-\tau_{i_n}) \quad (7)$$

$$+\varphi^{n-1}_{dyn}(\hat{\bar{u}}_n,(i_{n-1},I),t,\vec{\tau}_{(i_{n-1},I)})\delta(\bar{x}-\hat{\bar{u}}_n)\delta(t-\tau_{i_n}))\delta_{ii_n} \quad (8)$$

Here φ_{dyn} is the contribution of the dynamic events in eq. (3) (i.e. through the second term of the rhs of eq.(2)) On the other hand , for any function $\Gamma(\bar{u})$

$$\int d\bar{x}\int d\bar{u}\ \varphi(\bar{u},t,(i_n,I),\vec{\tau}_{(i_n,I)}))\delta(\bar{x}-\bar{g}_{i_n}(t-\tau_{i_n},\bar{u}))\delta(\bar{u}-\bar{u}_n)\Gamma(\bar{u}) = \varphi^n_{ET}(\bar{u}_n,(i_n,I),t,\vec{\tau}_{(i_n,I)})\Gamma(\bar{u}_n) \quad (9)$$

and then eq.(3) reads, after integrating over x and using eq.7

$$\varphi^n_{ET}(\bar{x}_n,(j_n,J),t,\vec{\tau}_{(j_n,J)}) = \sum_I \int_0^{\tau_{j_n}} d\tau_{j_{n-1}} \int_{\tau_{j_{n-1}}}^{t} d\tau \left(\prod_G \int_o^{\tau} d\tau^I_G\right) \times \quad (10)$$

$$(\varphi^n_{ET}(\bar{u}_n,(j_n,I),\tau,\vec{\tau}_{(j_n,I)})Q^{IJ}_{j_n,j_n}(t,\vec{\tau}_{(j_n,J)};\tau,\bar{u}_n,\vec{\tau}_{(j_n,I)})) \quad (11)$$

$$+(\varphi^{n-1}_{dyn}(\hat{\bar{u}}_n,(j_{n-1},I),\tau,\vec{\tau}_{(j_{n-1},I)})Q^{IJ}_{j_{n-1},j_n}(t,\vec{\tau}_{(j_n,J)};\tau,\hat{\bar{u}}_n,\vec{\tau}_{(j_{n-1},I)}))) \quad (12)$$

The first term accounts for activation events and the second for dynamic events . In the first term we have included failures of dynamic events that in practice behave as activation events. This equation may be solved iteratively , starting with stimulus activated during the first interval after the initiating event. Because this initiating event is assumed to occur instantaneously, we have at time zero

$$\varphi^1_{ET}(\bar{x}_1,(\vec{j}_1,J),t,\vec{\tau}_{(\vec{j}_1,J)}) = \pi(\bar{u}_0,(i_0,I_0),t)\bar{Q}^{I_0}_{i_0j_1}\Omega_{i_0j_1}(I_0\to J)\delta(t)\delta(\vec{\tau}_{(j_1,J)})\delta(\bar{x}_1-\bar{u}_o) \quad (13)$$

where $\bar{Q}^{I_0}_{i_0j_1}$ is the frequency of the initiating event, the omega factors accounting for the consequential changes in the initial state of the stimuli.

3.1.1 Exceedance frequency and sequence frequency

The paths and sequences that characterize the PSA approach allows us to use as the basic figure of merit the so called exceedance frequency. In order to model it within the SDTDP framework we first define a damage generation rate, $DG_p(\bar{x})$, such that $DG_p(\bar{x})$ is the damage of type p per unit time that is generated by the dynamic system at $\bar{x}$. Then the exceedance frequency of a damage D of type p is defined by

$$\nu^{exc}(D_p) \equiv \lim_{t\to\infty}\sum_{n,\vec{j}_n,I}\int d\vec{\tau}_{(j_n,I)}\varphi^n_{ET}(\bar{x}_n,(j_n,I),t,\vec{\tau}_{(j_n,I)}))\theta(\int_0^t d\tilde{\tau}DG_p(\bar{u}_{\vec{j}_n}(\tilde{\tau},\vec{\tau}_{j_n}))-D_p) \quad (14)$$

As for the sequence frequency

$$\nu(\vec{i}_n) \equiv \lim_{t\to\infty} \sum_I \int d\vec{\tau}_{(i_n,I)} \varphi^n_{ET}(\bar{x}_n, (i_n, I), t, \vec{\tau}_{(i_n,I)}) \tag{15}$$

4 Conclusions

A sequence approach, variant of the stimulus driven theory of probabilistic dynamics (SDTPD), eliminates drawbacks in current TPD dynamic approaches to probabilistic risk assessment, alowing to compute the exceedance frequency under the same assumptions of PSA. A description has been given of a set of equations that provide it in a consistent manner. SemiMarkovian and Markovian TPD has been shown to be nonrealistic particular cases.

Acknowledgements

The authors dedicate the present extension of the theory of probabilistic dynamics to the memory of Professor Jacques Devooght, whose intellectual influence is perceptible throughout the paper.

They are also indebted to Enrique Melendez and Javier Hortal, for his valuable input via numerous discussions.

References

Bley D., Kaplan S., Johnson D., 1992. The strengths and limitations of PSA: Where we stand. Rel. Engng. Syst. Safety 38, pp. 3-26.

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

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. **112**, pp. 101-113.

Devooght J., Smidts C., 1996. Probabilistic dynamics as a tool for dynamic PSA. Rel. Eng. Syst. Safety **52**, pp. 185-196.

Labeau P.E., Izquierdo J.M., 2004. Modeling PSA problems. I The stimulus driven theory of probabilistic dynamics. II A cell-to-cell transport theory approach. Accepted for publication in Nuclear Science and Engineering.

Siu N., 1994. Risk assessment for dynamic systems: An overview. Rel. Eng. Syst. Safety **43**, pp. 43-73.

Smidts C., 1992. Probabilistic reactor dynamics. IV. An example of man/machine interaction. Nucl.Sci.Eng. **112**, pp. 114-126.