INTEGRATED DETERMINISTIC AND PROBABILISTIC SAFETY ANALYSIS: CONCEPTS, CHALLENGES, RESEARCH DIRECTIONS

Enrico Zio

INTEGRATED DETERMINISTIC AND PROBABILISTIC SAFETY ANALYSIS: CONCEPTS, CHALLENGES, RESEARCH DIRECTIONS

Enrico Zio

EcoleCentrale Paris and Supelec, Chair on System Science and the Energetic challenge, European Foundation for New energy – Electricite de France (EDF), Grande Voie des Vignes 92295, Chatenay-MalabryCedex, France; email: enrico.zio@ecp.fr, enrico.zio@supelec.fr
Dipartimento di Energia, Politecnico di Milano, Via Ponzio 34/3 – 20133 Milano, Italy; email: enrico.zio@polimi.it

Abstract

Integrated deterministic and probabilistic safety analysis (IDPSA) is conceived as a way to analyze the evolution of accident scenarios in complex dynamic systems, like nuclear, aerospace and process ones, accounting for the mutual interactions between the failure and recovery of system components, the evolving physical processes, the control and operator actions, the software and firmware.

In spite of the potential offered by IDPSA, several challenges need to be effectively addressed for its development and practical deployment. In this paper, we give an overview of these and discuss the related implications in terms of research perspectives.

1. Introduction

In the Strategic Research Agenda (SRA)of the Sustainable Nuclear Technology Platform (SNETP) of the European Union, issued in May 2009,significant relevance is given to the safety of current and future Light Water Reactors (http://www.snetp.eu/www/snetp/images/stories/Docs-AboutSNETP/sra2009.pdf). Traditionally, regulation of design and operation of nuclear power plants have been based on deterministic analysis methods to verify criteria that assure plant safety in a number of postulated design basis accident scenarios. These criteria also allow identifying which plant Structures, Systems and Components (SSC) and activities are important to safety. Design, operation and maintenance of these "safety-related" SSC and activities are controlled through regulatory requirements.

However, compliance with the evolving regulatory requirements is anticipated to require innovative deterministic and probabilistic approaches of safety assessment for the existing nuclear power plants. In this respect, a related medium-term challenge explicitly mentioned in the SRA is to combine the use of deterministic and probabilistic methodologies for safety assessment.

The motivation for this comes from the realization that the static logic models (typically, event trees (ET) and fault trees (FT)) used in probabilistic safety assessment (PSA) have limitations in the modeling and treatment of the time-dependent interactions that shape dynamic accident scenarios, involving the failure and recovery processes of the system components, the physical processesevolving in the system, the control and operator actions, the software and firmware.

For example, in systems with multiple top events (TE), the actual final state of a dynamic scenario depends on the order, timing and magnitude of the component failure events (Aldemir, 1989; Hassan and Aldemir, 1990; Kirschenbaum et al., 2009; Zio and Di Maio, 2009; Zio et al., 2010); the static ET/FT approach, where the order of events is pre-set by the analyst, is not capable of capturing this and may fail to analyze vulnerable sequences which would, then, remain uncovered.

Accounting for dynamic process failures in digital instrumentation and control (I&C), and passive systems also poses a challenge to the static ET/FT analysis approach because failure can occurdue to the uncertain process behavior, even if no system components fail.

Finally, the impact of human operator actions along an accident sequence is also difficult to model with the traditional ET/FT approach to safety analysis.

In this context, the presentpaper tries toposition the concept of Integrated Deterministic and Probabilistic Safety Assessment (IDPSA) and discussesthe challenges for its development and deployment in practice.

In the following Section, we give a very brief overview of the methods for IDPSA. In Section 3, we list and discuss some of the main challenges for the use of these methods. In Section 4, we conclude with some comments on these challenges from a research perspective.

2. IDPSA Methodologies

IDPSA comprises a set of methods which use tightly coupled probabilistic and deterministic approaches to address aleatory (stochastic aspects of accident scenarios) and epistemic (model and parameters) uncertainties in a consistent manner (Aldemir, 2013).

A number of methodologies have been developedfor combining probabilistic and deterministic approaches to safety analysis in order to account for the time-dependentcharacter of the events which define accident progression.In these methodologies, the sequencing of events is not predetermined by the analyst (as it is the case with the traditional PSA modelling by ET/FT) but rather it emerges from the solution of the system model (usually simulated via a computer code) as the system evolves in time.

In the report (NUREG/CR-6901, 2006), a number of dynamic methodologies for probabilistic safety analysis are reviewed with regard to their applicabilityfor modeling digital systems in nuclear power plant PSA. Methodologiesincluded in the analyses are Markov modeling, dynamic flowgraph modeling and Petri net approaches. The reportalso points out the issues that need to be addressed, in both modeling the reliability of digital I&Csystems and incorporating digital I&C system reliability models into existing PSA models todetermine the overall plant response. Preliminaryacceptance criteria for digital system models prior to their implementationin regulatory applications are also introduced.

In the follow-up reports NUREG/CR-6942 and 6985, a benchmark Digital Feedwater ControlSystem (DFWCS) is specified and two dynamic methodologies, namely dynamic flowgraph methodology (DFM,NUREG/CR-6465; NUREG/CR-6710) and the Markov/Cell-to-cell mapping technique (CCMT,

Tombuyes and Aldemir, 1996 and 1997), are implemented todemonstrate how an existing nuclear power plant PSA canincorporate a digital upgrade of the instrumentation and control system. The results obtainedfrom the DFM and Markov/CCMT models of the DFWCS failure modes are compared, and theimpact of scenarios directly related to the hypothetical digital upgrade on the core damagefrequency (CDF) is assessed on a demonstrative basis. The study showsthat a DFWCS similar to that of an operating plant can be modeled using dynamicmethodologies and that the results can be incorporated into an existing PSA to quantify theimpact of a digital upgrade on the plant CDF.

Similarly, in the project Approdyn (final report in French downloadable athttp://hal.archives-ouvertes.fr/docs/00/74/01/81/PDF/Rapport_final_APPRODYN_v7a_NB.pdf, in French) different methods have been considered, including Stochastic and Synchronized Petri Nets, Stochastic Hybrid Automata and Piecewise Deterministic Markov Processes, for the analysis of a 900 MW Heat Exchanger with Steam Generator model provided by Electricite' de France (EDF).

A recent review of methodologies for IDPSA can be found in (Aldemir 2013), where they are categorized as: continuous-time, discrete-time and hybrid, i.e. considering both continuous and discrete times. The constitutive ingredients of all these methodologies are a time-dependent, physical model of the system dynamics, a list of identified, possible normal and abnormal system configurations and a model of the stochastic process of system transport in time from one state to another. Some methodologies have also graphical interfaces, an aspect which is regarded important for rendering feasible their use in practical applications.

Comprehensive continuous-time methodsinclude:

- the continuous event tree (CET) approach (Devooghtand Smidts, 1992a,b; Smidts and Devooght, 1992; Smidts, 1992), in which an integral equation is formulated to describe the system transport process in time accounting for dependencies amongfailure events due to process/hardware/software/firmware/humaninteractions; the problem is generally solved usingMonte Carlo simulation.
- The CCMT mentioned above, which defines the system states in terms of both system configurations (i.e., the vectors of the discrete states occupied by the components) and (user-specified) intervals (cells) "occupied" by the physical process variables. This allows modelling system configuration (instantaneous) changes upon crossings of threshold values (e.g. a valve opening when the pressure variable exceeds a given value). A continuous time Markov model describes the time-evolution of the probability of occupying the system states, in which the state transition rates are obtained from the system model and the Chapman–Kolmogorov equation; the problem can be solved using standard ordinary differential equation solvers.
- The stimulus-driven theory of probabilistic dynamics (Labeau and Izquierdo, 2005), which is capable of overcoming the limitation of the assumption of instantaneous changes in the system dynamics when a threshold is overcome or stimuli conditions prompt action for a change in the system (e.g. an operator action): changes may take some time to occur, and both the delay and the stimuli could be stochastic variables; the integral equation describing the process is solved by Monte Carlo methods.

Continuous-time methods are computationally intensive and the models and algorithms must be developed specificto the system under consideration: for these reasons, application has been limited.

Discrete-time methods are based on Monte Carlo simulation of the branching of scenarios (changes in system configuration) at the discrete times of occurrence of the stochastic events (e.g. component failures), followed by the deterministic simulation of the system process evolution by a physical model. For reducing the computational burden, biasing techniques to accelerate the stochastic simulation and meta-models (e.g. neural networks) to accelerate the deterministic simulation of the system process can be introduced. Examples are given in (Marseguerra et al., 1994; Marseguerra et al., 1995; Marseguerra and Zio, 1995, 1996, 1998; Labeau, 1996, 2006; Zio, 1995). For practical applications, the most promising discrete-time method is that of dynamic event trees (DET), which are ET whose scenario branching is not preset by the analyst: both the timing and sequence of the events occurring in a scenario are simulated from a time-dependentmodel of the system evolution with given branching conditions, which leads to amore comprehensive and systematic coverage of the space of possible event sequencesthan the traditional ET/FT approach. DET-based methods are DYLAM (Dynamical Logical Methodology) (Amendola and Reina,1984; Cacciabue et al., 1986; Cojazzi, 1996), DETAM (Dynamic EventTree Analysis Method) (Deoss and Siu, 1989), DDET (Dynamic DiscreteEvent Tree) (Acosta and Siu, 1993) method, ADS (AccidentDynamic Simulator) (Kae-Sheng and Mosleh, 1996), ISA (Integrated Safety Assessment)methodology (Izquerdo et al., 1994) , ADAPTapproach (Hakobyan et al., 2008; Catalyurek et al., 2010), MCDET whichuses both DETs and MC simulation (Marchand et al., 1998; Hoferet al., 2002; Hofer et al., 2004), GA-DPRA (Voroyev and Kudinov, 2011) which enables an intelligent andadaptive exploration of the scenario space. These methods differ in the way that branching is performed and controlled, in the different dynamic aspects modeled (including human interventions, passive systems, controls) and in the treatment of epistemic and aleatory uncertainty. These methods have been developed into software for nuclear application, with limitations coming from the computational burden and the processing of the large amount of data generated.

As previously mentioned, there are also methods with graphical interfaces, like Petri nets (Dutuitet al., 1997; Gribaudo et al., 2006), dynamic flowgraphs (Guarroet al., 1996; Yau, 1997), dynamic fault-trees (Andrews and Dugan,1999; Cepin and Mavko, 2001), the event-sequence diagram (ESD)approach (Swaminathan and Smidts, 1999), and the GO-FLOWmethodology (Matsuoka and Kobayashi, 1988, 1991).

3. Challenges for IDPSA methodologies

IDPSA is not intended to be used in replacement of Probabilistic Safety Assessment (PSA) and Deterministic Safety Assessment (DSA) approaches; rather, IDPSA is to be considered a way to:

- Explicitly account for time-dependent interactions between physical phenomena, equipment failures, safety and non-safety systems interactions, control logic, operator actions.

- Reduce expert judgment and simplifying assumptions about the above mentioned time-dependencies and the related scenarios structuring.
- Identify and characterize undiscovered plant vulnerabilities, i.e. a-priori unknown vulnerable scenarios (Figure 1).
- Treatdifferent sources of uncertainties, both aleatory and epistemic, in a coherent framework, for realistic quantification of safety margins with associated uncertainty estimation. IDPSA is expected to provide additional help to PSA and DSA practitioners and experts, by reducing and quantifying uncertainties in a consistent and resource- and time-efficient manner, as well as assuring proper coverage of the uncertainty space.

Figure 1 below abstractly sketches the contribution of IDPSA in identifying vulnerable scenarios. Given the unknown risk profile which the plant is subject to, risk analysis is used to estimate it and risk management to eventually envelope it with safety margins for protecting from the unknowns. Deterministic safety analysis (DSA) does so by considering conservative design basis accidents within a precautionary principle viewpoint against the potential threats; PSA attempts to more realistically follow the true risk profile, e.g. by an analytical ET/FT approach to identify minimal cut sets and accident scenarios. The integration of DSA and PSA enlarges the exploration of the possible plant scenarios by giving due account to time-dependencies in their development and the consistent treatment of uncertainties, with the possibility of uncovering unknown vulnerable scenarios.

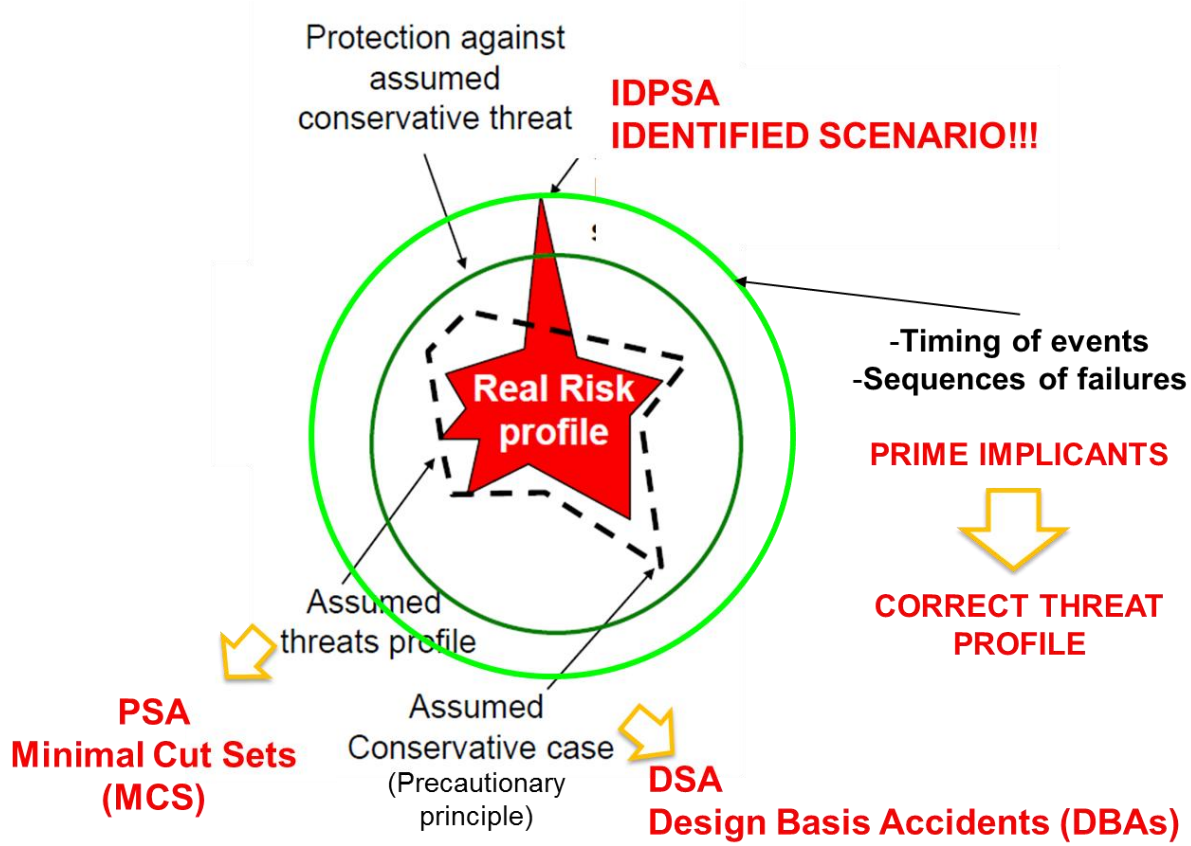

Figure 1: Representative sketch of the identification of undiscovered plant vulnerabilities by IDPSA = DSA (Deterministic Safety Analysis) + PSA (Probabilistic Safety Analysis). Prime implicants are the

extension of minimal cut sets which enable to account for the timing and sequencing of events occurrence; they are defined as event product terms (intersection of events) that render true the structure function and that cannot be covered by more generalimplicants, i.e., they cannot contain any shorter intersection of events that can render true the system structure function (Quine, 1952).

The benefits expected from IDPSA come at the price of new issues and challenges. While IDPSA, in principle, enlarges the exploration of the possible scenario space by avoiding to pre-set the ordering of events and including the time-dependencies interactions of all elements in the systems, its degree of completeness still depends on the plant basic event space, whose definition partly comes from PSA/DSA studies but a consistent way must be defined. This is complicated by the current situation of:

- Non-transparency of complex PSA models aiming at a realistic representation of complex system designs, when attempting at resolving time-dependent interactions between physical phenomena, control logic, operator actions, software/firmware and equipment failures.
- Increased complexity of the thermal-hydraulic (TH) models for DSA, with prohibitive computational costs for running hundreds/thousands of transients simulations with Best-Estimate (BE) deterministic codes.
- Difficult quantification of the uncertainties associated to the TH modelsadopted for accident analysis in DSA.
- Increased complexity in the assessment of the impact of human operator actions on time-dependent scenarios.

While IDPSA is recognized to potentially complement traditional DSA and PSA with an improved coverage of the uncertain risk profile and increased capabilities of modelling hardware/software/process/human interactions during scenario evolution, in practice it is important that this can be achieved in consistency with the existing methods and tools of DSA and PSA to which they should “add-on” and not “replace”. This is a most critical aspect for deployment to industry, and includes the need for flexible computational platforms allowing for linking of different codes, with their input-output requirements and structures.

From the computational point of view, the burden of scenario generation is dramatically increased in IDPSA. To reduce computational burden,developments are undergoing for:

- Efficient parallel processing of scenarios (Catalyurek et al., 2010).
- Early pruning of branches in the dynamic event trees, e.g. based on their probability (Cojazzi, 1996) or on their similarity with scenarios of no interest for the analysis (the non-failure scenarios) (Zamalieva et al., 2013).
- Use of advanced Monte Carlo simulation methods (i.e. Line Sampling and Subset Sampling) and meta-models (i.e., Neural Networks, Support Vector Machines, Local Gaussian Processes) mimicking best-estimate (BE) codes, to efficiently simulate the large number of accidental sequences necessary, to cover the long periods of time required by the analysis and also to discover rare events of interest (Marseguerra et al. 1994, 1995; Pedroni et al., 2010; Zio and Pedroni 2009, 2010, 2011; Zio et al., 2010).Resorting to advanced Monte Carlo simulation (Zio, 2013) is necessary for the estimation of the (very low) probabilities of

the(rare) failureevents of interest, since a crude Monte Carlo would require a very large number of runsof the BE code of the TH model, with prohibitive computational times in practice. Still, the computational times could remain impractical even when resortingto advanced Monte Carlo simulation methods, if the BE code were required to be more accurate and detailed: in this case, meta-modelling could be the only viable solution.Meta-models are compact scalable models that approximate the multivariate input/output behaviour of complex systems and processes, based on data from a limited set of experimental observations or computationally expensive simulations. Their use is constantly increasing for parametric studies, design and scenario space exploration, uncertainty and sensitivity analysis, optimization. They are also called surrogate models, response surface models (RSM), emulators, auxiliary models, repro-models, etc. Interestingly, recently effective strategies for further reducing computational efforts of complex systems scenarios evaluations have been proposed, which combine Monte Carlo-based methods with meta-modelling (Echard et al., 2011; Bourimet et al., 2011; Doubourg et al, 2013; Echard et al., 2013; Cadini et al., 2014).

At the back-hand of the IDPSA analysis, the challenge is to be able to handle and manipulate the massive amount of scenario data generated in a transparent post-processing capable of allowing the assimilation of the contained information by PSA and DSA. In particular within a Monte Carlo simulation framework for IDPSA, the information on the evolution of the system is hidden in the system life histories that are simulated as part of the computational procedure. Among these histories, there are sequences that reproduce qualitatively similar behaviours in terms of the evolution of the physical parameters and of the sequences of events of state transition, mainly differing for the times at which these latter occur. Other sequences may instead differ in behaviour, because characterized by different combinations of occurred events, and still reach the same final outcome state. The difficulty in identifying and grouping similar scenarios lies in the fact that same event sequences may correspond to rather different process parameters evolutions and, possibly, end states, depending on the events timing or on their occurrence order. Then, grouping the scenarios only on the basis of the occurred events and end states may not be sufficient and accountancy of the physical behaviour of the process variables should also be included.In this respect, a number of methods are being proposed, based on clustering of the scenario data (Figure 2) (Podofillini et al., 2008; Zio and Di Maio, 2009; Mandelli et al., 2010; Di Maio et al., 2011).

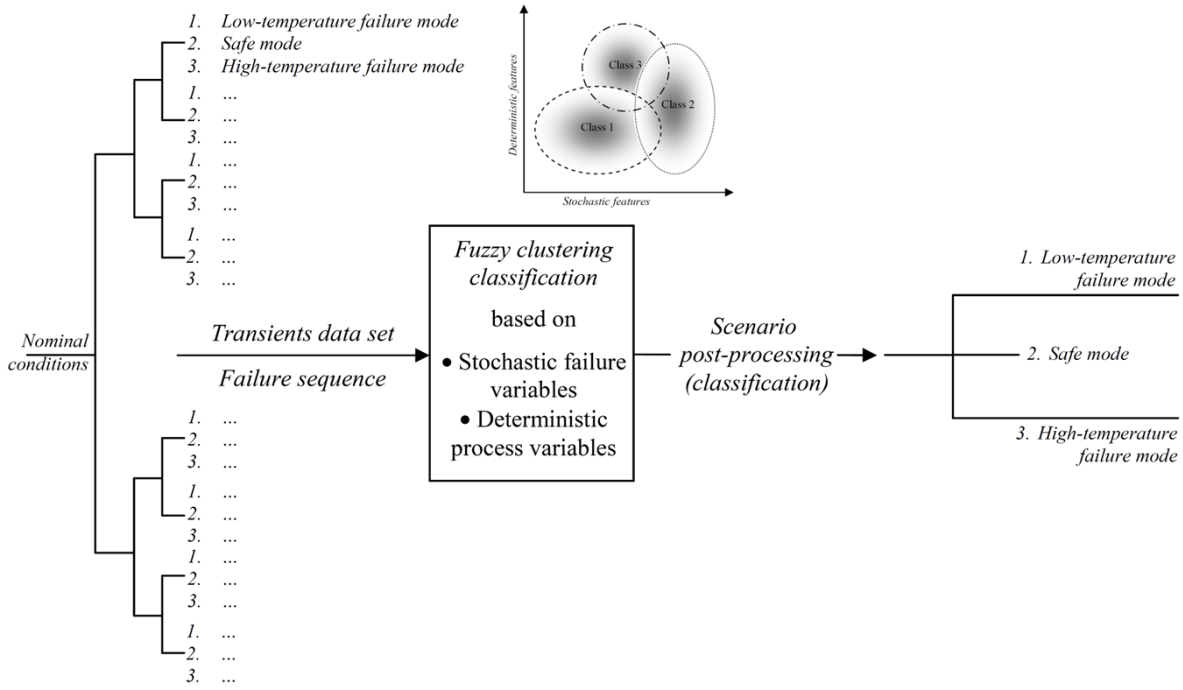

Figure 2: Conceptual scheme of IDPSA scenario post-processing for a case of multiple failure modes (low-temperature and high-temperature failure modes): scenario classification by fuzzy clustering based on the values of the characteristic variables of the stochastic events and deterministic process (Zio and Di Maio, 2011).

The underlying idea of these approachesis to group the IDPSA-generated scenarios in classes of "similarity", by combining information from both the event sequences and the patterns of evolution of the process variables.In all generality, this leads to a task of pattern classification, i.e. the partitioning of objects into classes. In particular,a classification algorithm can be built through a process of learning based on a set of patterns labelledwith the class they belong to: this kind of techniques is termed "supervised" and the available pre-classified data are termed "training" data.

For IDPSA post-processing purposes, the first step is the a priori identification of the anticipated scenario classes for the system under analysis and of the relevant classification features. The scenarios will eventually be classified as belonging to a particular class based on the affinity of their features to those characteristic of the class. Scenario classes should distinguish different reference scenarios that the system is expected to follow in its evolution. They must be defined a priori on the basis of available knowledge on the system operation. For example, classes of scenarios may be 1) the nominal operative scenarios; 2) scenarios involving the non-automatic startup of the High Pressure Injection (HPI) system; 3) scenarios involving both the non-automatic startup of HPI and the failure of a Turbine Bypass Valve (TBV). The identification of the features relevant to the classification is necessary to condense the scenario description into an object vector x, i.e. the pattern to be fed to the classification function. The features can be either binary or continuous variables. Binary variables characterize the scenarios based on the occurrence or not of certain events, for example the intervention or failure of a safety system; continuous variables characterize the scenario based on the evolution of the process variables.

The successive steps of the procedure are typical of a supervised classification scheme: training of the classifier on patterns of known classes and test of the classifier on new patterns.

Once the IDPSA scenarios are classified properly, the probability of each class can be estimated and the dominant evolutionary patterns identified, in terms of both failure events sequences and process variables evolutions.

An important asset sought from thesepost-processing techniques is related to the capability of recognizing unanticipated scenarios, i.e. patterns of evolution that were not foreseen as reference in the a priori analysis and thus do not fall in any scenario class. The identification of new, unforeseen evolutionary patterns completes the analyst knowledge on the system with information on unexpected failure scenarios, i.e. undiscovered plant vulnerabilities, and may aid to suggest additional and more effective safety-oriented improvements of the system.

Finally, a fundamental issue for allowing the use of IDPSA in industrial practice is an improvement in the usability of IDPSA codes by non-developers: user-friendly graphical interfaces for the development of the input structure and for the post-processing of the output results are needed, accompanied by proper training for use.

4. Conclusions

The strive for very low risk levels in highly hazardous technologies like nuclear, oil and gas, aerospace, etc.is challenging the state-of-the-art safety analyses (PSA / DSA)due to the increase use of passive safety systems in new plants and retrofits in existing plants, the introduction of I&C, the need to consider the role of the human operators in the scenarios development, the implementation of severe accident management in plant design. These newly added ingredients significantly complicate the analysis and introduce additional uncertainties, thus rendering difficult a solid “a priori” judgment about conservatism in the selected DSA and PSA scenarios.

IDPSA is considered to be the way to go to complement PSA/DSA in response to these challenges. Overcoming of the limitations of PSA/DSA is achieved by the use of both in their respective applicability domains, via an integration which leads to a more complete exploration of the scenario space and coverage of undesired events, with the consistent treatment of the different sources of uncertainty involved in the analysis, both aleatory and epistemic.

IDPSA provides a framework for analysing and simulating directly the response of a system to an initial perturbation, as the system hardware and software components and the operating crew interact with each other and with the environment. This can be achieved by embedding models of controlled process dynamics and human operator behaviour within stochastic simulation engines reproducing the occurrence of failure and success transitions along the scenarios.

This way of system modelling goes beyond the classical approach to PSA which relies on techniques, such as ET/FT, to represent the analyst understanding of the system logic with respect to its failure mechanisms. Such classical approach to system analysis requires significant pre-processing efforts for the analyst to acquire the detailed knowledge of the integral system logic and dynamics necessary to structure the accidental scenarios into the proper discrete logic frame. In some situations this way of

approaching the problem fails to capture and reproduce salient features of the system behaviour. A typical case is when differences in the sequence order of the same success and failure events along an accident scenario affect its outcome. Another case is when the timing of occurrence of the events along the scenario substantially affects its evolution and possibly its outcome. Finally, modellingand analysis difficulties are encountered when the evolution of the process variables (temperatures, pressures, mass flows, etc …) affects the occurrence probabilities of the events and, thus, the subsequent scenario evolution.

To cope with these issues, IDPSA methodologies attempt to integrate dynamic and stochastic processes to capture the integrated dynamic response of the system hardware and process, the control and operator actions, the software and firmware, during an accident scenario. In this framework, the analyst is somewhat relieved from the pre-processing task of identifying the accident scenarios, which are instead automatically generated within the dynamic simulation.

On the other hand, by this way the number of scenarios that are analysed is much larger than that of the classical ET/FT logic approaches, so that not only the computational burden is increased but also the a posteriori information retrieval and interpretation becomes more difficult.

On the other hand, the IDPSA approach brings several potential advantages. First, there is the possible identification of accident scenarios which may have been overlooked by the analyst in the pre-processing phase. Second, conservative simplifying assumptions made by the analyst, for example on the evolution of some process parameters, can be relaxed as the process evolution is simulated directly by the underlying dynamic model. Finally, additional informative insights are gained from the analysis, in the form of time-dependent joint probability density functions of components states and process parameters values. In this respect, again, the amount of information retrievable from IPDSA analyses, in terms of number of scenarios and probability distributions, can be overwhelming and generally calls for a significant effort in the post-processing phase. Yet, retrieving the dominant scenarios of the system dynamic evolution can provide significant safety and risk-informed insights on the criticality of the scenarios and on the efficiencies of the protections designed to counteract them.

In this sense, IDPSA can contribute significantly torobust risk-informed decision making in safety, by allowing for both probabilistic and deterministic considerations in the analysis of the mutual, time-dependent interactions of the stochastic process of hardware component failures, the deterministic response of the system process, the effects of the control and operator actions, software and firmware.

Methods are continuously being developed and improved, with the aim to bring IDPSA to industrial practice. This entails:

- Computational efficiency for the generation of the multiple scenarios of interest (the failure ones), by both efficient stochastic (by advanced Monte Carlo) and deterministic (by advanced meta-modelling) simulations.
- Efficient and transparent post-processing (by clustering and data mining) of the analysis output, to render it usable.
- User-friendliness of the IDPSA code in the input and at the output, and flexibility of the computational platform for allowing the link with existing PSA/DSA codes.

References

Acosta, C., Siu, N., 1993. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. Reliability Engineering and SystemSafety 41, 135–154.

Aldemir, T., 1989. Quantifying setpoint drift effects in the failure analysis of processcontrol systems. Reliability Engineering and System Safety 24, 33–50.

Aldemir, T., 2013. A survey of dynamic methodologies for probabilistic safety assessmentof nuclear power plants, Annals of Nuclear Energy 52, 113–124.

Amendola, A., Reina, G., 1984. DYLAM-1, A Software Package for Event Sequenceand Consequence Spectrum Methodology. EUR-924, CEC-JRC ISPRA,Commission of the European Communities, Ispra, Italy.

J.-M. Bourinet, F. Deheeger, M. Lemaire, "Assessing small failure probabilities by combined subset simulation and Support Vector Machines". Structural Safety 2011; 33: 343-353

Cacciabue, P.C., Amendola, A., Cojazzi, G., 1986. Dynamic logical analyticalmethodology versus fault tree: the case of auxiliary feedwater system of anuclear power plant. Nuclear Technology 74, 195–208.

Catalyurek, U., Rutt, B., Metzroth, K., Hakobyan, A., Aldemir, T., Denning, R.S.,Dunagan, S., Kunsman, D., 2010. Development of a code-agnostic computationalinfrastructure for the dynamic generation of accident progressionevent trees.Reliability Engineering and System Safety 95, 278–304.

Cepin, M., Mavko, B., 2001. A dynamic fault-tree. Reliability Engineering and SystemSafety 75, 83–91.

Cojazzi, G., 1996. The DYLAM approach to the dynamic reliability analysis ofsystems. Reliability Engineering and System Safety 52, 279–296.

Deoss, D., Siu, N., 1989. A Simulation Model for Dynamic System AvailabilityAnalysis. M.S. Thesis, MIT Department of Nuclear Engineering, Boston,Massachusetts.

Devooght, J., Smidts, C., 1992a. Probabilistic reactor dynamics I: the theory ofcontinuous event trees. Nuclear Science and Engineering 111, 229–240.

Devooght, J., Smidts, C., 1992b. Probabilistic reactor dynamics – III: a framework fortime dependent interaction between operator and reactor during a transientinvolving human error. Nuclear Science and Engineering 112, 101–113.

F. Cadini, F. Santos, E. Zio, "An improved adaptive Kriging-based importance sampling for sampling multiple failure regions of low probability". Under revision. 2014.

F. Di Maio, P. Secchi, S. Vantini, E. Zio, "Fuzzy C-Means Clustering of Signal Functional Principal Components for Post-Processing Dynamic Scenarios of a Nuclear Power Plant Digital Instrumentation and Control System", IEEE Transactions on Reliability, Volume 60, no. 2, pp. 415-425, June 2011.

V. Dubourg, B. Sudret, F. Deheeger, “Metamodel-based importance sampling for structural reliability analysis”. Probabilistic Engineering Mechanics 2013; 33: 47-57.

Dutuit, Y., Chatelet, E., Signoret, J.-P., Thomas, P., 1997. Dependability modeling andevaluation by using stochastic Petri nets: application to two test cases.Reliability Engineering and System Safety 55, 117–124.

B. Echard, N. Gayton, M. Lemaire, “AK-MCS: An active learning reliability method combining Kriging and Monte Carlo Simulation”. Structural Safety 2011; 33:145-154.

B. Echard, N. Gayton, M. Lemaire, N. Relun, “A combined Importance Sampling and Kriging reliability method for small failure probabilities with time-demanding numerical methods”. Reliability Engineering and System Safety 2013; 111:232-240.

Gribaudo, M., Horvaacute, A., Bobbio, A., Tronci, E., Ciancamerla, E., Minichino, M., 2006. Fluid Petri nets and hybrid model-checking: a comparative case study.Reliability Engineering and System Safety 81, 239–257.

Guarro, S., Yau, M., Motamed, M., 1996. Development of Tools for safety Analysis ofControl Software in Advanced Reactors. NUREG/CR-6465, US NuclearRegulatory Commission, Washington, DC.

Hassan, M., Aldemir, T., 1990. A data base oriented dynamic methodology for thefailure analysis of closed loop control systems in process plants. ReliabilityEngineering and System Safety 27, 275–322.

Hofer, E., Kloos, M., Krzykacz-Hausmann, B., Peschke, J., Woltereck, M., 2002. Anapproximate epistemic uncertainty analysis approach in the presence ofepistemic and aleatory uncertainties. Reliability Engineering and SystemSafety 77, 229–238.

Hofer, E., Kloos, M., Krzykacz-Hausmann, B., Peschke, J., Sonnenkalb, M., 2004.Dynamic Event Trees for Probabilistic Safety Analysis. GRS, Garsching,Germany.

Izquerdo, J.M., Hortal, J., Sanches-Perea, J., Melendez, E., 1994. Automatic generationof dynamic event trees: a tool for integrated safety assessment. In: Aldemir, T.,Siu, N., Mosleh, A., Cacciabue, P.C., Goktepe, B.G. (Eds.), Reliability and SafetyAssessment of Dynamic Process Systems, NATO ASI Series F, vol. 120. Springer-Verlag, Heidelberg, pp. 135–150.

Kae-Sheng, H., Mosleh, A., 1996. The development and application of the accidentdynamic simulator for dynamic probabilistic risk assessment of nuclear powerplants. Reliability Engineering and System Safety 52, 297–314.

Kirschenbaum, J., Bucci, P., Stovsky, M., Mandelli, D., Aldemir, T., Yau, M., Guarro, S., Ekici, E., Arndt, S.A., 2009. A benchmark system for comparing reliabilitymodeling approaches for digital instrumentation and control systems. NuclearTechnology 165, 53–95.

Labeau, P.E., Izquierdo, J.M., 2005. Modeling PSA problems – I: the stimulus-driventheory of probabilistic dynamics. Nuclear Science and Engineering 150, 115–139.

Mandelli, D., Aldemir, T., Yilmaz, A., 2010a. Scenario aggregation in dynamic PRAuncertainty quantification. Transactions of the American Nuclear Society 103,371–374.

Mandelli, D., Metzroth, K., Yilmaz, A., Denning, R.S., Aldemir, T., 2010b. Probabilistic clustering for scenario analysis. Transactions of the American Nuclear Society103, 371–374.

Marchand, S., Tombuyes, B., Labeau, P., 1998. DDET and Monte Carlo simulation tosolve some dynamic reliability problems. In: Mosleh, A., Bari, R. (Eds.), PSAM 4.Springer-Verlag, New York, pp. 2055–2060.

M. Marseguerra, M. Nutini, E. Zio: Approximate Physical Modelling in Dynamic PSA Using Artificial Neural Networks, Reliability Engineering and System Safety, vol. 45, pp. 47 - 56, 1994.

M. Marseguerra, E. Zio, The Cell-To-Boundary Method in Monte Carlo-Based Dynamic PSA, Reliability Engineering and System Safety, vol. 48, pp.199-204, 1995.

M. Marseguerra, M. Ricotti, E. Zio, Approaching System Evolution in Dynamic PSA by Neural Networks", Reliability Engineering and System Safety, vol. 49, pp. 91-99, 1995.

M. Marseguerra and E. Zio, Weight Updating In Forced Monte Carlo Approach To Dynamic PSA, Monte Carlo Methods, 4, N 4, 1998, pp. 359-374.

Matsuoka, T., Kobayashi, M., 1988. GO-FLOW: a new reliability analysismethodology. Nuclear Science and Engineering 98, 64–78.

Matsuoka, T., Kobayashi, M., 1991. An analysis of a dynamic system by the GOFLOWmethodology. In: Cacciabue, P.C., Papazoglou, I.A. (Eds.), ProbabilisiticSafety Assessment and Management. Elsevier, New York, pp. 1436–1547.

NUREG/CR-6465, 1996. Development of Tools for Safety Analysis ofControl Software in Advanced Reactors. US NuclearRegulatory Commission, Washington, DC.

NUREG/CR-6710, 2001. Extending the Dynamic FlowgraphMethodology (DFM) to Model Human Performance and Team Effects., US Nuclear Regulatory Commission, Washington, DC.

NUREG/CR-6901, 2006.Current State of ReliabilityModeling Methodologies forDigital Systems and TheirAcceptance Criteria forNuclear Power Plant AssessmentsUS Nuclear Regulatory Commission, Washington, DC.

NUREG/CR-6942, 2007. Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk AssessmentsUS Nuclear Regulatory Commission, Washington, DC.

NUREG/CR-6985, 2009. A Benchmark Implementation ofTwo Dynamic Methodologies forthe Reliability Modeling of DigitalInstrumentation and ControlSystemsUS Nuclear Regulatory Commission, Washington, DC.

N. Pedroni, E. Zio, G.E. Apostolakis, “Comparison of bootstrapped Artificial Neural Networks and quadratic Response Surfaces for the estimation of the functional failure probability of a thermal-hydraulic passive system”, Reliability Engineering and System Safety, 95(4), pp. 386-395, 2010.

Podofillini, L., Zio, E., Mercurio, D., Dang, V.N., 2008. Dynamic safety assessment:scenario identification via a fuzzy clustering approach. Accident Analysis andPrevention 41, 1180–1191.

Quine W.V., The problem of simplifying truth functions, Am. Math. Monthly, Volume 59, 521-531, 1952.

Swaminathan, S., Smidts, C., 1999. The mathematical formulation of the eventsequence diagram framework. Reliability Engineering and System Safety 65,103–118.

Tombuyes, B., Aldemir, T., 1996. Dynamic PSA of process control-systems viacontinuous cell-to-cell-mapping. In: Cacciabue, P.C., Papazoglou, I.A. (Eds.), Probabilistic Safety Assessment and Management. Springer-Verlag, New York,pp. 1541–1546.

Tombuyes, B., Aldemir, T., 1997. Continuous cell-to-cell mapping. Journal of Soundand Vibration 202, 395–415.

Voroyev, Y., Kudinov, P., 2011. Development and Application of a Genetic AlgorithmBased Dynamic PRA Methodology to Plant Vulnerability Search. PSA 2011,American Nuclear Society, LaGrange Park.

Yau, M., 1997. Dynamic Flowgraph Methodology for the Analysis of Software BasedControlled Systems. Ph.D. Thesis, University of California, Los Angeles.

Zamalieva, D., Yilmaz, A. and Aldemir, T., 2013. A probabilistic model for online scenario labeling in dynamic event tree generation, Reliability Engineering and System Safety, Volume 120, December 2013, Pages 18–26.

E. Zio. The Monte Carlo Simulation Method for System Reliability and Risk Analysis. Springer, 2013.

E. Zio: Biasing the Transition Probabilities in Direct Monte Carlo, Reliability Engineering and System Safety, vol. 47, pp.59-63, 1995.

E. Zio, F. Di Maio, “A Data-Driven Fuzzy Approach for Predicting the Remaining Useful Life in Dynamic Failure Scenarios of a Nuclear Power Plant”, Reliability Engineering and System Safety, RESS, 10.1016/j.ress.2009.08.001, 2009.

E. Zio, F. Di Maio, M. Stasi, “A data-driven approach for predicting failure scenarios in nuclear systems”, Annals of Nuclear Energy, 37, 482–491, 2010

E. Zio and N. Pedroni, "Estimation of the Functional Failure Probability of a Thermal-Hydraulic Passive System by Subset Simulation", Nuclear Engineering and Design, vol 239, No. 3, 2009, pp. 580-599.

E. Zio and N. Pedroni, "Functional Failure Analysis of a Thermal-Hydraulic Passive System by Means of Line Sampling", Reliability Engineering and System Safety, vol 9, No. 11, pp. 1764-1781, 2009.

E. Zio, N. Pedroni, "An optimized Line Sampling method for the estimation of the failure probability of nuclear passive systems", Reliability Engineering and System Safety, doi: 10.1016/j.ress.2010.06.007.

E. Zio, N. Pedroni, “How to effectively compute the reliability of a thermal-hydraulic passive system”, accepted for publication on Nuclear Engineering and Design, Volume 241, Issue 1, pp. 310-327, Jan. 2011.

E. Zio, N. Pedroni, M. Broggi, L. Golea, “Modelling the dynamics of the Lead Bismuth Eutectic eXperimental Accelerator Driven System by an Infinite Impulse Response Locally Recurrent Neural Network”, Nuclear Engineering and Technology, 41(10), pp. 1293-1306, 2009.

E. Zio, F. Di Maio, “Processing Dynamic Scenarios from a Reliability Analysis of a Nuclear Power Plant Digital Instrumentation and Control System”, Annals of Nuclear Energy, doi:10.1016/j.anucene.2009.06.012, 2009.