Aldemir Tunc
The Ohio State University, Columbus, Ohio, U.S.A.

Dynamic methodologies for reliability and probabilistic risk assessment (PRA)

Keywords

reliability, dynamic methodologies, probabilistic risk assessment

Abstract

Dynamic methodologies in reliability and PRA are those that explicitly account for the time element in probabilistic system evolution. Dynamic methodologies are usually needed when the system has more than one failure mode, control loops, and/or hardware/process/ software/human interaction. An overview of the dynamic methodologies proposed to date is given, including those that use dynamic event tree generation, continuous time-state space representation, the cell-to-cell mapping technique and graphical schemes. The use of dynamic methodologies for state/parameter estimation in on-line applications is also discussed. Potential on-line use of dynamic methodologies as operator assistance tools for risk informed accident management or normal operation is described and illustrated.

1. Introduction

Starting in the late 1970's, numerous concerns have been raised on the capability of static approaches to dynamic process system failure modeling (such as a conventional event-tree/fault-tree approach) on a stand-alone basis [31], [9], [25], [10], [17], [2], [3] and various methodologies have been proposed which explicitly account for the time element in system evolution to complement the static approaches[2], [32]. Often referred to as dynamic methodologies, these methodologies have shown that the undesirable event (Top Event) frequencies, as well as the structure of minimal cut sets leading to these Top Events, can be quite sensitive not just to the order but also to the exact timing of the component failure or human intervention/non-intervention, time constants of the process and uncertainties in the process physics.

In 1992, a North Atlantic Treaty Organization (NAT O) Advanced Research Workshop (ARW) on the Reliability and Safety Analysis of Dynamic Process Systems was held in Turkey to discuss the advantages and limitations of the dynamic methodologies proposed to date, as well as to identify practical situations where the dynamic methodologies could lead to significantly improved results[6]. The ARW was attended by a total of 33 participants representing 26 different institutions including universities, national laboratories, private consulting companies and regulatory bodies. The participants' combined expertise covered nuclear, chemical, mechanical, aerospace and defence systems. Some of the participants were directly involved in the development of dynamic methodologies; others were experts in conventional risk assessment applications. No strong consensus was reached during the ARW as to precisely when dynamic methodologies should be used. However, the participants were in general agreement that dynamic methodologies not only need to be further investigated but also the investigations need to be accelerated, including comparison of dynamic methodologies with others on a sample standard problem with characteristics similar to that discussed in [2] and later exercised in [20] and [37]. An important attempt in this direction was the preparation of a special issue of Reliability Engineering & System Safety on the Reliability and Safety Assessment of Dynamic Process Systems (Volume 52, June 1996) which presents work that provides a formal methodological framework for many of the dynamic methodologies proposed to date [23] and shows some features of the dynamic methodologies vis-à-vis classical techniques [19], as well as addressing computational issues [12] which continue to be a limitation in the implementation of dynamic methodologies.

In spite of these efforts, the static event-tree/fault-tree methodology [44] is still the most popular system reliability modeling technique due to the simplicity in use and clarity in communicating the results of the analysis. Recently, attention has refocused on dynamic methodologies due to the potential need for them in the nuclear, aerospace and aviation industries and a benchmark system has been specified to test the capabilities of dynamic methodologies proposed for the risk modeling of digital instrumentation and control systems in nuclear power plants [7]. This paper gives a brief survey of dynamic methodologies with regard to their advantages and limitations in the probabilistic risk modeling of engineering systems (prognostic methods), as well as their potential use as operator assistance tools for risk informed accident management or normal operation (diagnostic/prognostic methods).

2. Prognostic methods

In making predictions regarding the response of a system to disturbances, both the uncertainties arising from the stochastic nature of events (aleatory uncertainties) as well as those arising from lack of knowledge about the processes relevant to the system (epistemic uncertainties) have to be taken into account. Often, it is difficult to distinguish between epistemic and aleatory uncertainties [13]. Dynamic methodologies allow a unified framework to account for both types of uncertainties simultaneously in predicting the distribution of risk associated with the system response.

Dynamic methodologies can be divided into three main categories: (i) continuous-time methods, (ii) discrete-time methods, and (iii) methods with visual interfaces [5]. Continuous-time methods such as the continuous event tree (CET) approach [21] yield the probability of finding the system at a specified location in the system state-space at a specified time in a specified configuration. In CET, this probability is calculated from the solution of an integral equation whose inputs are the physical process model in a differential or integral form and transition rates between system hardware states. A discrete state-space version of CET is the continuous cell-to-cell-mapping (CCCM) method [43]. The CCCM defines the system states as consisting of hardware configurations and user specified intervals of the physical process variables (cells). The probability evolution of system states the cell space is modeled using a continuous time Markovian representation. The state transition rates are obtained from the user provided system model and the Chapman-Kolmogorov equation.

Discrete-time methods include the following [5]:

- DYLAM (Dynamical Logical Methodology) [19], [8] is the first methodology proposed to generate dynamic event trees. In essence, it is a simulation driver able to generate branchings (scenarios) of system evolution at user specified time intervals and to coordinate the simulation of every branch. For each scenario, a time dependent probability is evaluated. Any undesired consequence is identified from the generated scenarios and its probability is calculated by adding up the probabilities of contributing branches.
- DETAM (Dynamic Event Tree Analysis Method) [20], DDET (Dynamic Discrete Event Tree) method [36] and ADS (Accident Dynamic Simulator) [30] are three variants of DYLAM which can dynamically generate at each time step all the possible event trees. Branches with small probability are pruned based on some user input threshold to prevent the number of simulations to be performed from becoming unmanageable. The ISA (Integrated Safety Assessment) methodology [29] only branches every time a setpoint for system intervention is crossed or an action needs to be taken by the system or the operator, in general. The underlying assumption in ISA is that the likelihood of failure on demand dominates erroneous activation or deactivation of continuously operating systems and leads to fewer branches to be followed.
- Monte-Carlo (MC) simulation approach of [37], [33], [34] uses discrete time sampling to investigate possible branchings in the system evolution due to component malfunction and follows the branches to calculate the probability/frequency of undesirable events.
- DDET/MC hybrid simulation as described in [36] generates the branchings with a DDET engine and selects the branches to be followed by the MC approach.
- CCMT (Cell-to-Cell Mapping Technique) [2], [28], [4] is based on a discrete time version of CCCM and follows the probabilistic evolution of the system using a Markov chain. The CCMT results can be formulated as dynamic event trees [14] or dynamic fault trees [15] and subsequently can be incorporated into a conventional PRA using the event-tree/fault-tree methodology [16].

Methods with visual interfaces include [5] Petri nets [7], [26], dynamic flowgraphs [27], [46], dynamic fault-trees [18], [11], the event-sequence diagram (ESD) approach [42], and the GO-FLOW Methodology [38], [39]. In a manner similar to fault-tree analysis, visual models based on Petri nets can be constructed to represent cause-and-effect relationships among events and yield minimal cut sets. Unlike fault-tree analysis, a Petri net model allows explicit representation of the time element in the system evolution with the use of a dynamic system model and subsequently is capable of simulation of concurrent and dynamic activities and time-delays. The dynamic flowgraph methodology (DFM) is a digraph-based technique. A process variable is represented by a node discretized into a finite number of states. The system dynamics is represented by a cause-and-effect relationship between these states. Instead of minimal cut sets, the DFM yields the prime implicants for the system. A prime implicant is any monomial (conjunction of primary events) that is sufficient to cause the top event, but does not contain any shorter conjunction of the same events that is sufficient to cause the top event. Dynamic fault-trees use timed house events [18] or functional dependency gates [11] to represent the time varying dependencies between basic events. Quantification of dynamic fault-trees is performed using time dependent Boolean logic [18] or Markov models [11]. The ESD approach uses 6-tuple of events (e.g., initiating, pivotal, delay), conditions (e.g., limiting time, competition, switch), gates (multiple input AND/OR, multiple output AND/OR), process parameter set, constraint and dependency rules to represent the probabilistic system evolution. The events represent transitions between system states. The probabilistic approach is an extension of the CET [21] approach and is based upon the Chapman-Kolmogorov equation. The output is the probability of being in a given system state as a function of time. Both cyclic and acyclic scenarios can be identified and quantified. The GO-FLOW methodology is a success-oriented system analysis technique, capable of evaluating system reliability and availability. The modeling technique produces the GO-FLOW chart, which consists of signal lines and operators. The operators model function or failure of the physical equipment, a logical gate, and a signal generator. Signals represent some physical quantity or information. The analysis is performed from the upstream to the downstream signal lines, and is completed when the intensities of the final signals at all time points are obtained. GO-FLOW output includes time dependent system reliability/availability, cut sets, common cause failure analysis and, uncertainty analysis.

3. Diagnostic/prognostic methods

In accident management or even in normal operation it is important to be able to predict the likelihood of possible future states of the system. Nuclear power plants use risk monitors which provide a real time analysis tool that can be used to determine the level of risk from the plant, based on the actual status of systems, components and the activities being carried out on the plant [47]. The main use of risk monitors is as an on-line tool to monitor and control the risk from the plant configurations that arise during normal plant operation, calculate and monitor the allowed configuration time as the plant configuration changes (provided as input), and monitor the cumulative risk. They are also used for maintenance planning to ensure that maintenance activities are carried out in a way that prevents the occurrence of large peaks in the risk and restricts the cumulative risk over a period of time to an acceptable level.

Risk monitors use the plant PRA model which is based on the static fault-tree/event-tree approach. Very few studies have been encountered in the available literature that would allow incorporation of the impact of the process dynamics into the prediction of the future plant states. For such an application, an accurate knowledge of the system state is essential. On the other hand, the available instrumentation in the system rarely provides complete information on the state of the system and a coupling of diagnostic and prognostic methods are needed for the predictions.

An adjoint version of the CET approach [22] could be used as a diagnostic tool to estimate the probability distribution of plant states that could lead to the observed plant state which then can be input to CET to predict the likelihood of the possible future system states. While conceptually sound, there has not been an implementation of this approach on practical systems.

The approach described in [40] uses the DSD (Dynamic System Doctor) as a prognostic tool to estimate the probability distribution of the unobserved system state variables [45] and the ISA methodology to generate dynamic event trees to predict the probability distribution of future system states. The DSD is based on the CCMT approach for the representation of system dynamics. However, rather than using a forward Markovian model, it uses an adaptive Bayesian approach to look back in time to estimate the probability distribution of the unobserved system state variables. Some useful features of this approach are the following:

- It estimates a lower and an upper bound for the unobserved state variables/parameters, as well as the expected values of these variables/parameters. Such bounds are important for determining the safety margins during operation.
- It can account for uncertainties in the monitored system state, inputs and modeling uncertainties through the appropriate choice of the cells. It also provides a measure to rank the likelihood of faults in view of these uncertainties.
- It allows flexibility in system representation. Differential or difference equations as well as almost any type of input/output model (e.g. neural net) can be used to generate the cell-to-cell transition probabilities.

- The discrete-time nature of the methodology is directly compatible with a look-up table implementation which is very convenient for the use of data that may be available from tests or actual incidents.
- For diagnostics, it does not require model inversion (which may lead to singularity problems) or inverse models (which usually have limited range of applicability).

4. Conclusion

Dynamic PRA methodologies provide capabilities to overcome the limitations of the conventional static approaches when there are hardware/software/firmware/process/human interactions in the system. Approaches have been proposed that can be used as purely off-line prognostic tools or on-line diagnostic/prognostic tools. The diagnostic/prognostic tools may reduce the risk in the operation of safety critical systems by allowing the operators to predict the consequences of the actions taken during accident management. The current challenges in the use of dynamic methodologies are: a) the need for general-purpose, user-friendly interfaces, and, b) meeting the computational demand for practical applications.

References

[1] Acosta, C. & Siu, N.(1993). *Dynamic Event Trees in Accident Sequence Analysis: Application to Steam Generator Tube Rupture*, 135-154.

[2] Aldemir, T. (1987). Computer-Assisted Markov Failure Modeling of Process Control Systems. *IEEE Transactions on Reliability*, R-36:133-144.

[3] Aldemir, T. (1989). Quantifying Setpoint Drift Effects in the Failure Analysis of Process Control Systems. *Reliability Engineering & System Safety*, 24:33-50.

[4] Aldemir, T. (1991). *Utilization of the Cell-To-Cell Mapping Technique to Construct Markov Failure Models for Process Control Systems.* In: Apostolakis G ed. Elsevier, New York, 1431-1436.

[5] Aldemir, T., Miller, D. W., Stovsky, M., Kirschenbaum, J., Bucci, P., Fentiman, A. W. & Mangan, L. M. (2006). *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*. U. S. Nuclear Regulatory Commission, Washington, D.C.

[6] Aldemir, T., Siu, N., Mosleh, A. & Cacciabue, P. C. (1994). *Reliability and Safety Assessment of Dynamic Process Systems*. Springer-Verlag, Heidelberg.

[7] Aldemir, T., Stovsky, M.,P., Kirschenbaum, J., Mandelli, D., Mangan L. A., Miller, D. W., Fentiman, A. W., Ekici, E., Guarro, S., Yau, M., Johnson, B., Elks, C. & Arndt, S. A., (2007). *Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments*. U.S. Nuclear Regulatory Commission, Washington, D.C.

[8] Amendola, A. & Reina, G. (1984). DYLAM-1, A Software Package for Event Sequence and Consequence Spectrum Methodology, ISPRA, Commission of the European Communities.

[9] Andow, P. K. (1980). Difficulties in fault-tree synthesis for process plants. *IEEE Trans Reliability*, R-27:1-9.

[10] Andow, P. K. (1981). Fault Trees and Failure Analyses: Discrete State Representation Problems. Transactions *IChemE - Chemical Engineering Research and Design*, 59a, 125-128.

[11] Andrews, J. D. & Dugan, J. (1999). Dependency Modeling Using Fault-Tree Analysis. *The System Safety Society*, Unionville, Virginia, 67-76.

[12] Belhadj, M. & Aldemir, T. (1996). Some Computational Improvements in Process System Reliability and Safety Analysis Using Dynamic Methodologies. *Reliab Engng & System Safety*, 52, 339-347.

[13] Belhadj, M., Hassan, M. & Aldemir, T. (1992). On the Need for Dynamic Methodologies in Risk and Reliability Studies. *Reliab Engng & System Safety*, 38, 219-236.

[14] Bucci, P., Kirschenbaum, J., Aldemir, T., Smith, C. L. & Wood, T. S. (2006). *Constructing Dynamic Event Trees from Markov Models.* In: Stamataletos M, Blackman HS eds. ASME Press, Inc.

[15] Bucci, P., Kirschenbaum, J., Aldemir, T., Smith, C. L. & Wood, R. T. (2006). *Generating Dynamic Fault Trees from Markov Models.*

[16] Bucci, P., Mangan, L. A., Kirschenbaum, J., Mandelli, D., Aldemir, T. & Arndt, S. (2006). Incorporation of Markov Reliability Models for Digital Instrumentation and Control Systems into Existing PRAs. *American Nuclear Society, La Grange, IL.*

[17] Cacciabue, P. C., Amendola, A. & Cojazzi, G. (1986). Dynamic logical analytical methodology versus fault tree: The case of auxiliary feedwater system of a nuclear power plant. *Nucl Technol*, 74, 195-208.

[18] Cepin, M. & Mavko, B. (2001). *A Dynamic Fault-Tree, Reliab Engng & System Safety*, 75, 83-91.

[19] Cojazzi, G. (1996). The DYLAM Approach to the Dynamic Reliability Analysis of Systems. *Reliab Engng & System Safety*, 52, 279-296

[20] Deoss, D. & Siu, N. (1989) *A Simulation Model for Dynamic System Availability Analysis.* M.I.T. Department of Nuclear Engineering, Boston, Massachussets.

[21] Devooght, J., Smidts, C. (1992). Probabilistic Reactor Dynamics I: The theory of continuous event trees, *Nucl Sci Engng,*112, 229-240.

[22] Devooght, J. & Smidts, C. (1992). Probabilistic reactor dynamics - III: A framework for time dependent interaction between operator and reactor during a transient involving human error. *Nucl Sci Engng*, 112, 101-113.

[23] Devooght, J., Smidts, C. (1996). Probabilistic dynamics as a tool for dynamic PSA. *Reliab Engng & System Safety*, 52, 185-196.

[24] Dutuit, Y. (1997). *Dependability Modeling and Evaluation by Using Stochastic Petri Nets: Application to Two Test Cases,* 117-124.

[25] Galluzo, M. & Andow, P. K. (1998). Failures in Control Systems. *Reliability Engineering,* 7, 125-128.

[26] Gribaudo, M., Horvaacute, A., Bobbio, A., Tronci, E., Ciancamerla, E. & Minichino, M. (2006). *Fluid Petri Nets and Hybrid Model-checking: A Comparative Case Study*, 239-257.

[27] Guarro, S., Yau, M. & Motamed, M. (1996). *Development of Tools for safety Analysis of Control Software in Advanced Reactors, U.S. Nuclear Regulatory Commission,* Washington, D.C.

[28] Hassan, M. & Aldemir, T. (1990). A Data Base Oriented Dynamic Methodology for the Failure Analysis of Closed Loop Control Systems in Process Plants. *Reliability Engineering & System Safety*, 27, 275-322.

[29] Izquierdo, J. M., Hortal, J., Sanches-Perea, J. & Melendez, E. (1994). *Automatic Generation of Dynamic Event Trees: A Tool for Integrated Safety Assessment*. In: Aldemir T, Siu N, Mosleh A, Cacciabue PC, Goktepe BG eds. Springer-Verlag, Heidelberg, 135-150.

[30] Kae-Sheng, H. & Mosleh, A. (1996). The Development and Application of the Accident Dynamic Simulator for Dynamic Probabilistic Risk Assessment of Nuclear Power Plants. *Reliability Engineering & System Safety*, 52, 297-314.

[31] Kumamoto, H. & Henley, E. J. (1979). Safety and reliability synthesis of systems with control loops. *AICHE Journal*, 25, 108-113.

[32] Kumamoto, H., Henley, E. J. & Inoue, K. (1981). Signal-flow-based graphs for failure mode analysis of systems with control loops. *IEEE Trans Reliability*, R-30, 110-116.

[33] Labeau, P. (1996). Probabilistic Dynamics: Estimation of Generalized Unreliability through Efficient Monte Carlo Simulation. *Ann Nucl Energy*, 23, 1355-1369.

[34] Labeau, P. (2006). A survey on Monte Carlo estimation of small failure risks in dynamic reliability. *International Journal of Electronics and Communication*, 52, 205-211.

[35] Lajeunesse, S., Hutinet, T. & Signoret, J. P. (1996). *Automatical fault trees generation on dynamic systems.* In: Cacciabue PC, Papazoglou IA eds. Probabilistic Safety Assessment and Management, Springer-Verlag, New York, 1553-1559.

[36] Marchand, S., Tombuyes, B. & Labeau, P. (1998). DDET and Monte Carlo Simulation to Solve Some Dynamic Reliability Problems. In: Cacciabue PC, Papazoglou IA eds. Probabilistic Safety Assessment and Management, Springer-Verlag, New York, 2055-2060.

[37] Marseguerra, M. & Zio, E. (1996). Monte Carlo Approach to PSA for Dynamic Process Systems. *Reliability Engineering & System Safety,* 52, 227-241.

[38] Matsuoka, T. & Kobayashi, M. (1988). GO-FLOW: A New Reliability Analysis Methodology. *Nuclear Science and Engineerin*g, 98, 64-78.

[39] Matsuoka, T. & Kobayashi, M. (1991). *An Analysis of a Dynamic System by the GO-FLOW Methodology.* In: Cacciabue PC, Papazoglou IA eds. Probabilistic Safety Assessment and Management '96, Elsevier, New York, 1547-1436.

[40] Munteanu, I. & Aldemir, T. (2003). A Methodology for Probabilistic Accident Management. *Nucl Technol*, 144, 49-62.

[41] Senni S., Semenza S. M. & Galvani R. (1991). *A.D.M.I.R.A. - An analytical dynamic methodology for*
integrated risk assessment, In: Apostolakis G ed. Probabilistic Safety Assessment and Management, Elsevier Science Publishing Co., New York, 413-418

[42] Swaminathan S., Smidts C. (1999). *The Mathematical Formulation of the Event Sequence Diagram Framework,* 103-118.

[43] Tombuyes, B. & Aldemir, T. (1996). Dynamic PSA of Process Control-Systems Via Continuous Cell-To-Cell-Mapping, *Probabilistic Safety Assessment and Management PSAM3*. Elsevier, New York, 1541-1546.

[44] U. S. Nuclear Regulatory Commission. (1975). Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, In: WASH-1400 (NUREG-75/014) ed. US Nuclear Regulatory Commission, Washington, D.C.

[45] Wang, P., Chen, X. M. & Aldemir, T. (2002). DSD: A Generic Software Package For Model-based Fault Diagnosis in Dynamic Systems. *Reliability Engineering & System Safety*, 75, 31-39.

[46] Yau, M. (1997). *Dynamic Flowgraph Methodology for the Analysis of Software Based Controlled Systems.* University of California, Los Angeles.

[47] Nuclear Energy Ageny (2005). Technical Opinion Paper on the Development and Use of Risk Monitors at Nuclear Power Plants, Organization for Economic Co-Operation And Development. Paris, France