Development of Smart Component Based Framework for Dynamic Reliability Analysis of Nuclear Safety Systems

Darpan Krishnakumar Shukla[1], A. John Arul[2]

[1]Indira Gandhi Centre for Atomic Research, Homi Bhabha National Institute, Kalpakkam 603102, Tamil Nadu, India.
[2]Indira Gandhi Centre for Atomic Research, Kalpakkam 603102, Tamil Nadu, India.

E-mail contact of main author: darpanks@igcar.gov.in

Abstract: Dynamic reliability methodologies account for the safety system's time dependent characteristics while estimating the reliability. Time dependence can arise due to interdependence of process conditions and hardware states and action of control element. Though static reliability models often capture the average behavior and try to make conservative estimates, it is inadequate from a number of perspectives. First, this requires that the analyst needs to establish that the model is conservative. Second, such modeling requires more expertise and experience in the appropriate domain of the problem, rather than in the reliability methods. Third, approximate methods may be inadequate to establish reliability enhancements or degradations due to subtle alterations in the system design. In spite of the significant effort in the reliability community to establish dynamic reliability analysis methods, there are no general purpose tools similar to that available for fault tree event tree modeling. In this regard *Smart Component* based method is identified as a suitable candidate for general purpose dynamic reliability assessment and developed for implementation. Smart Component based dynamic method uses elements of object oriented architecture and Monte Carlo simulation and, is suitable for being developed into a general purpose tool. The paper demonstrates the capability of the method to evaluate reliability of systems having various types of time dependence, interaction between hardware failure and process evolution and complexity by means of few case studies. The method is found to be promising for accurate modeling of dynamic as well as static scenarios.

Key Words: Dynamic Reliability, Probabilistic Dynamics, Smart components and Monte Carlo Simulation

1. Introduction

Importance of safety in nuclear power plant is well known and the safety of the system is measured in terms of reliability of the system. Next generation nuclear power plants are increasingly using digital instrumentation and control (IC) systems for safe operation of plant and employ passive safety systems for performing critical safety functions. The digital IC systems are complex and highly interacting systems with the physical process and hardware. Estimation of reliability of the digital systems using traditional static methods require approximate modelling of the system and hence it has number of limitations: First, this requires that the analyst needs to establish that the model is conservative. Second, such modeling requires more expertise and

experience in the appropriate domain of the problem, rather than in the reliability methods. Third, approximate methods may be inadequate to establish reliability enhancements or degradations due to subtle alterations in the system design. For better modeling dynamic reliability methodologies have been developed. They are capable of modeling the problem of simultaneous stochastic hardware failure and dynamic process evolution dependent on the hardware state - known as probabilistic dynamics. The dynamic reliability methodologies should be able to model:

- change of system structure function with time
- time dependence of the reliability parameters (failure rate, mission time, test interval)
- Interaction effects: dependence of process variables on the hardware states and dependence of hardware states on process variables.

A number of dynamic reliability methodologies have been developed such as Cell to Cell Mapping Technique [1][2], Discrete Dynamic Event Tree [3] [4][5][6], Dynamic Fault Tree [7][8][9], Dynamic Flowgraph Methodology[10] [11], Petri Nets [12][13], Event Sequence Diagram [14][15], Stochastic Hybrid Automaton [16][17][18], GO-Flow methodology [19], Dynamic Bayesian Network [20][21][22][23], Monte Carlo methodology [24][25][26][27], etc. These methods are reviewed in ref. [28][29][30]. Globally, there is no consensus on a dynamic reliability method being developed into a general purpose tool with proof-of-concept and user friendly features.

Smart component methodology uses the elements of object oriented architecture for component and system representation. Monte Carlo methods are used to evaluate the representation for reliability, which can easily incorporate various types of time dependence, interaction between hardware failure and process evolution [31][29]. The smart component based methodology is having an easy input representation scheme and it has user friendly feature. In this method, user need not to define/store all states and there is no need to define all event scenarios. In this approach, the same system representation can be reused for both static and dynamic studies [29]. The method can be easily incorporated into present PRA. Hence, smart component based methodology embedding Monte Carlo simulations schemes is chosen for further development. The paper develops a Smart Component based dynamic methodology and demonstrate feasibility of the method to solve the reliability problems of critical nuclear safety systems with dynamic aspects.

Subsequent section 2. develops the smart component methodology that is able to model the above mentioned requirements and outlines simulation procedure. Further, the method is demonstrated for static reliability estimation of an active redundant system and unavailability calculations of a simple dynamic tested system, and results are discussed in section 3.. Finally the contribution of the paper is concluded in section 4..

2. Smart Component Methodology

The Smart Component Methodology (SCM) is a simulation based dynamic reliability method with object oriented input representation. In this study we have used a data base for the system representation, consisting of 1) all the components as tables of the data base, and 2) a relationship between components as a connector table (see Figure 1). The object-as-a-component have

attributes of the actual component and it behaves like the component. The attributes of the component includes state of the components' hardware, reliability parameters, process variables, laws of the component-describing the exact behaviour of the component, input variables and output variables, safety criteria for one or more process variables, control threshold, etc. The list of the attributes is not exhaustive. In general, attributes are classified as input, output, state (constant state or dynamic state) or reliability data. The hardware state, process variables, safety criteria, control threshold are described in the object as state. Each attributes are defined with values and assignment of the values to these attributes is straight forward i.e., it corresponding to the actual phenomena. The values are accessed and edited at any point of time and it describe the current state of the component. The attributes are also able to model dependencies or relationships with other components; the relations are defined in a relational table of the data base.

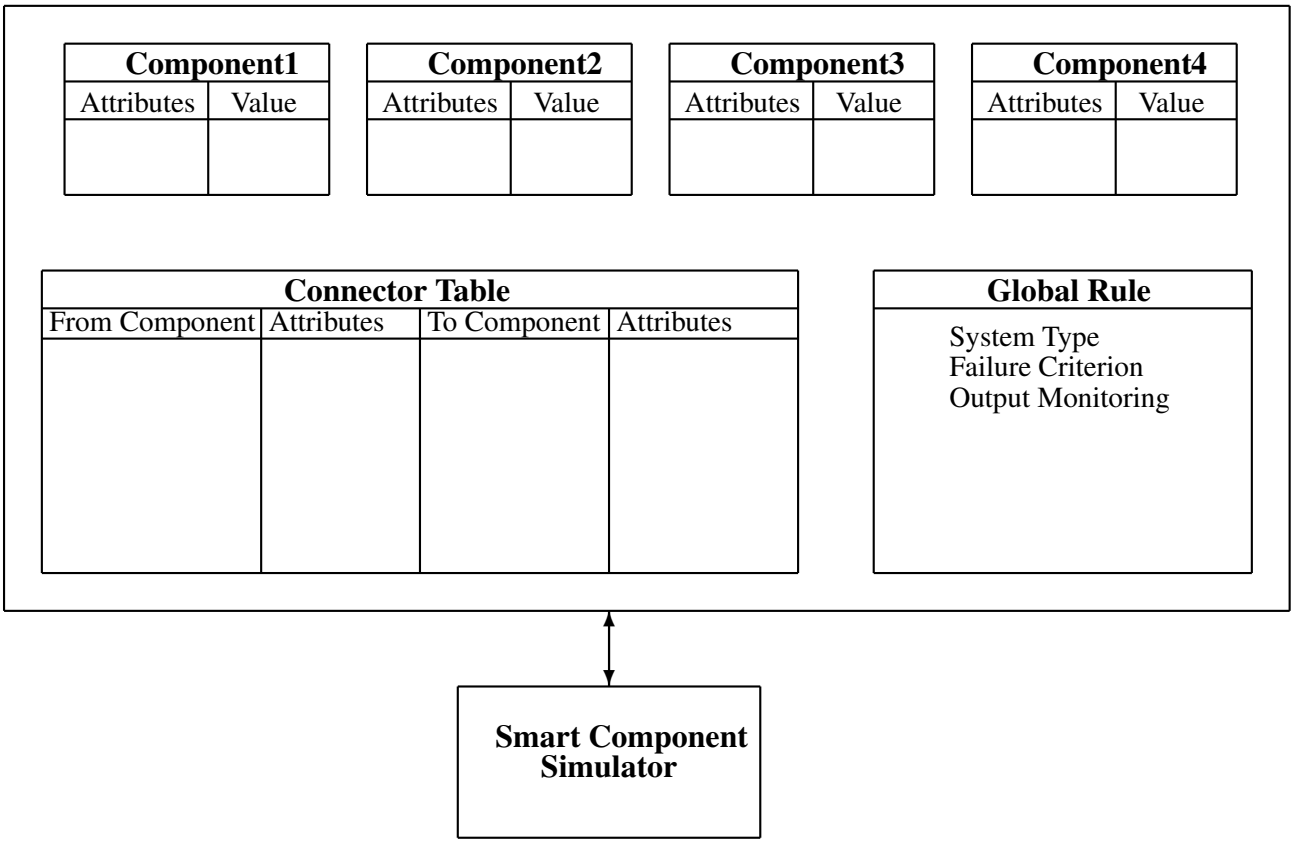

Figure 1: Smart Component Framework

A connector table describes explicitly the hard wiring between the components and the attributes of the interrelated or dependent components common to both. Each entries in connector table describes the attributes with which the component is connected to the attributes of the other component. The connection represents either a binary signal, a non-binary signal for process sequence, or a control signal generated by one component. Hence, any type of component dependency or in-dependency and interactions between hardware failure and process evolutions are modelled using these relationships. The communication occurring between the components of the dynamic system is facilitated through the connector table.

The behaviour of the component is as important as describing the interrelationships. The behaviour of the component in the system is described in the Smart Component methodology

as a law of the component. The detail of a law of the component represents the detail of the modelling. According to the values of input variables, states of the component and reliability parameters, the execution of the law causes change in the values of the output variables, the states of the system or other dependent component states. The output variables may be a linear/differential function of input variables, states and/or time. While executing a law of one component other components' attributes are un-altered. To depict the simulation of the dynamic system the execution of laws of the components is carried out in a specific ordered sequence. The process of going from input to the output or to the delivering-end is well defined in the design of the system, and hence, the sequence of the components is a known parameter.

Once the system is described with all its components using a connector table and laws, Analog Monte Carlo simulation of the system is performed in the following manner: First, sampling of the time to transition using Markov Monte Carlo method described in ref. [24]. Second, the system is evolved/controlled up to the sampled time of transition by executing the sequence of laws of the components at each time step. Third, transition of the component state determined according to the Markov Monte Carlo method described in ref. [24]. The tallying of the system failure is carried out after every transition of the state for the defined system failure criteria. Importance sampling based variance reduction techniques such as forced transition and/or failure biasing can be applied for accelerated Monte Carlo calculations in step 1 and step 3 respectively. In accelerated Monte Carlo simulation the importance sampling is carried out up to first system failure subsequently analog Monte Carlo simulation sampling procedures are applied.

For static reliability estimation of the same system, the same system model can be utilized along with a reachability check up to the end component or function-delivering component from the starting component. The reachability check is started from each starting component and propagated towards the end component, if a failed component is found in between, then the path is terminated and other alternative path is followed. If the reachability up to the end component found then it is concluded that the system is in working state. If all the path are terminated due to one or more component failure then the system is in failed state. The reachability check is carried out after each component state transition. In the following section the application of the reachability concept in Smart Component methodology for static reliability estimation of an example system k/m active redundant system is demonstrated.

3. Application of Smart Component Methodology to Two Example Systems

3.1. Static Reliability Estimations of an Active Redundant System

Towards validating and performance checking for Smart Component based method simple examples are studied in this paper including static and dynamic evaluation. The redundancy increases the complexity in the system model in terms of dependency and size. A redundant system have more than one input components; and, to model this situation, Smart Component method treats the number of inputs easily using reachability check concept. It checks reachability to the end component, and if the reachability is achieved with more than required path (2 for 2/3 voting system) than the system is assumed to be in working state otherwise in failed state. With this, an example of a widely used 2/3 voting system is evaluated using Smart Component methodology below.

Three temperature sensors are distributed for monitoring temperature in a reactor safety system. Though one sensor is enough for temperature monitoring, three sensors are used for redundancy

purpose, and, two-by-three voting logic is used for decision purpose. Scram is actuated upon receiving of two scram signals from either of the three sensors. The system reliability parameters are estimated for unreliability for a specified mission time and unavailability using analog and accelerated Monte Carlo methods of the Smart Component methodology and Reliability Workbench 10.2, as described below. As shown in Figure (2), a voting system is connected to three sensors. The scram is actuated upon crossing of safety limit by two or more sensors. The reliability evaluation of the system is straight forward. The system database is built considering constant repairable model for each components and static reliability is estimated with failure criteria defined as: the failure of two or more input sensors. Failure rate of one sensor is higher 10^{-3} per hour and other sensors are having failure rates of 10^{-4} per hour. Repair rate of 10^{-1} per hour is same for all the three sensors.

Results and Discussion:

The reliability parameters such as steady state unavailability and mission time unreliability are estimated using Markov Monte Carlo simulation with both analog and importance sampling methods for the simple redundant system. The fault tree of the simple redundant 2/3 voting system evaluated using Reliability Workbench 10.2. The results are shown in Table I. The results shows that the analog and accelerated Monte Carlo techniques give accurate results and the results are matching satisfactorily. The fractional error and coefficient of variation indicate that the performance of accelerated simulation is very good.

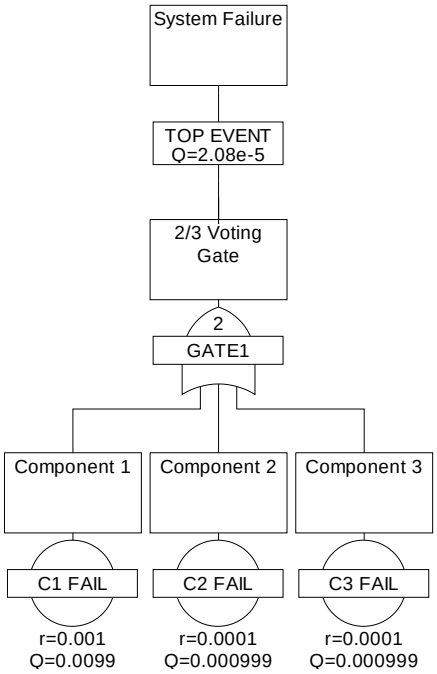

Figure 2: Fault Tree of the 2by3 Voting System

TABLE I: SMART COMPONENT RESULTS FOR COMPARISION OF RELIABILITY OF THE 2/3 REDUNDANT SYSTEM FOR MISSION TIME OF 1000 HR

Number of histories	N
Number of Batch	M
Average time per history (seconds)	$\bar{t}$
Unavailability	$\bar{A}$
Variance	σ_a^2
Fractional Error	$f_A = \frac{\sigma}{\bar{A}}$
Coefficient of Variation	$\Delta = N^{\frac{1}{2}} * f_A$
Figure of Merit	FOM=$\frac{1}{\sigma^2 \bar{t}}$
Unreliability	$\bar{R}$

Parameters	**Analog MC SCM**	**Accelerated MC SCM**	**Reliability Workbench 10.2**
N	10000	10000	
M	5	5	
$\bar{t}$	0.195	0.256	
$\bar{A}$ $(\times 10^{-5})$	1.8	1.	2.08
σ_a^2 $(\times 10^{-8})$	3.56	0.0078	
f_A	10.42	1.410	
Δ_A	1042.29	141.05	
FOM$_A$	1.44×10^8	5.08×10^9	
$\bar{R}$	0.0035	0.0039	0.0041
σ_r^2	3.5×10^{-7}	1.8×10^{-5}	
f_R	0.167	1.079	
Δ_R	16.73	107.88	
FOM$_R$	1.44×10^7	2.14×10^5	

3.2. Unavailability Estimation of an Simple Dynamic Tested System

For achieving high reliability redundancy at system level or at component level is used. The high reliability is also being achieved by employing testing and diagnosing system to the system. In the tested system, the system is tested periodically for its working conditions with a test interval. Upon detection of the failed condition a deterministic or probabilistic repair process is initiated and the repaired condition of the component is either 'as good as new', 'minimal repair'. Moreover, the tests can be of either Type I, Type II or of Type III as described in ref. [32]

In the direct Monte Carlo simulation of this situations, the time during which the system is down is dictated by the repair time and test interval. This dynamic situation cannot be modeled easily using traditional reliability methodology such as fault tree, event tree, reliability block diagram. Even though Markov models are successful for the unavailability calculations of the maintained systems (see Figure 4), because of the state space explosion problem, scalability of the model to complex system is doubtful. In this paper a tested/failure category [Told, Fold] and the Type II of scheduled maintenance as defined in [32] is modeled in Smart Component framework and quantitative analysis is performed for unavailability calculations. the approximate expression

for unavailability for the tested system as shown in Figure (3) is arrived at using Shanon Decomposition method as follows: Here, λ_i is failure rate, τ_i is testing interval and T_i is mean time to repair, where $i = s, d$. We can write the Shannon decomposition for two variable boolean function $f(D, S)$ as,

$$f(D, S) = D * f(1, S) + \bar{D} * f(0, S) \tag{1}$$

$$P(f(D, S)) \equiv P(D)P(S|D) + P(\bar{D})P(S|\bar{D}) \tag{2}$$

With rare event assumption, the probabilities are:

$$P(f(D, S)) \equiv \lambda_d(T_d + \tau_d)\lambda_s(T_d + \tau_d) + \lambda_s(T_s + \tau_s/2) \tag{3}$$

The schematic of the system is shown in Figure 3. A tested system is connected to a testing and diagnosing system. The testing system tests the tested system at specified time intervals. In [Told, Fold] category of maintenance neither tests nor repair have any effect on reliability characteristics of the components. In type II of scheduled maintenance a component is maintained periodically at constant intervals τ_s irrespective of any repairs which might have taken place before. And upon detection of the failed component a deterministic repair process is initiated. Here, the testing system is also manually tested with success probability of one at constant intervals τ_d. A constant mean time to repair model is used for repair of both the components with MTTR of $T_s(= \frac{1}{\mu_s})$ and $T_d(= \frac{1}{\mu_d})$. The failure rates are denoted by λ_s and λ_d per hour.

Results and Discussion:

Unavailability of the tested system is calculated after generalising the analog Monte Carlo method to SCM. Unavailability is also calculated using approximate unavailability obtained from Shanon expansion of equation 3, Markov model as given in Figure 4. The results for approximate method, Markov model and Smart Component Monte Carlo method are given in column 2,3 and 4 respectively in Table II. It is observed that the estimated unavailability value matches with the Markov model of the two component tested system, whereas the approximately calculated unavailability is always higher.

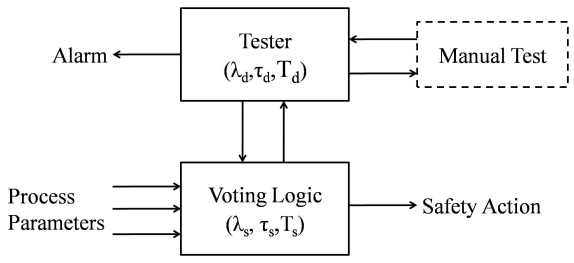

Figure 3: A Simple Tested System

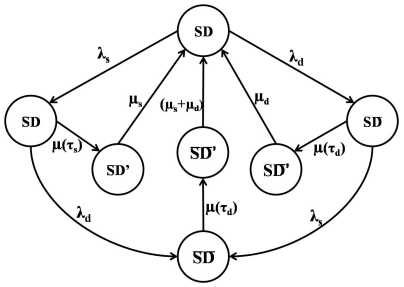

Figure 4: Markov model of the tested system

TABLE II: UNAVAILABILITY RESULTS OF THE TESTED SYSTEM

Parameters	**Approximate Method**	**Markov Model**	**Smart Component Methodology**
$\lambda_s = 1 \times 10^{-4}$ $\lambda_d = 1 \times 10^{-4}$ $\tau_s = 1hr$ $\tau_d = 24hr$ $T_s = T_d = 4hr$	$\bar{A} = 5.1 \times 10^{-4}$	$\bar{A} = 4.5 \times 10^{-4}$	$\bar{A}$= 4.5×10^{-4} N = 10000 M = 10 $\sigma^2 = 4.1 \times 10^{-10}$ $f = 0.045$ $\bar{t} = 0.00002sec$ $\Delta = 1.39 \times 10^{13}$

4. Conclusion

The object oriented representation based Smart Component method is developed for application to dynamic reliability problems. A relational data base framework is chosen for implementation. The method is applied to two example systems, viz, 1) an active redundant system for static reliability calculations and, 2) a simple tested system for dynamic reliability calculation. Application of accelerated Monte Carlo method is also demonstrated with SCM for achieving faster calculations with less error. The results of SCM for static reliability calculations are matching well with that from the traditional methods and the results for dynamic methods eliminate conservatism. The results of evaluation of SCM for dynamic and static reliability calculations gives confidence that it can be used to solve more complex problems while avoinding the state-space explosion problem encountered in Markov modeling. Further study is in progress to apply the method to industrial scale problems.

5. References

[1] M. Belhadj, T. Aldemir, The cell to cell mapping technique and Chapman-Kolmogorov representation of system dynamics, J. Sound Vib. 181 (4) (1995) 687–707. doi:10.1006/jsvi.1995.0166.

[2] T. Aldemir, Utilization of the cell to cell mapping technique to construct Markov failure models for process control systems, in: PSAM Meet., 1991.

[3] A. Amendola, G. Reina, DYLAM-1 A Software Package For Event Sequence And Consequence Spectrum Methodology, Tech. rep. (1984).

[4] C. G. Acosta, N. O. Siu, Dynamic Event tree analysis method (DETAM) for accident Sequence Analysis, Tech. rep. (1991).

[5] K.-S. Hsueh, A. Mosleh, The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants, Reliab. Eng. Syst. Saf. 52 (1996) 297–314.

[6] G. Cojazzi, The DYLAM approach for the dynamic reliability analysis of systems, Reliab. Eng. Syst. Saf. 52 (1996) 279–296.

[7] M. Čepin, B. Mavko, A dynamic fault tree, Reliab. Eng. Syst. Saf. (1) 83–91. doi:10.1016/S0951-8320(01)00121-1.

[8] J. B. Dugan, S. J. Bavuso, M. A. Boyd, Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems, IEEE Trans. Reliab. 41 (3) (1992) 363–377. doi:10.1109/24.159800.

[9] S. K. Shin, Y. G. No, P. H. Seong, Improvement of the Reliability Graph with General Gates to Analyze the Reliability of Dynamic Systems That Have Various Operation Modes, Nucl. Eng. Technol. 48 (2) (2016) 386–403. doi:10.1016/j.net.2015.12.002.

[10] K. Bjorkman, Solving dynamic flowgraph methodology models using binary decision diagrams, Reliab. Eng. Syst. Saf. 206–216doi:10.1016/j.ress.2012.11.009.

[11] T. Aldemir, D. W. Miller, M. P. Stovsky, J. Kirschenbaum, P. Bucci, A. W. Fentiman, L. T. Mangan, Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments (NUREG/CR-6901), Tech. rep.

[12] C. Cordier, M. Fayot, A. Leroy, A. Petit, Integration of process simulations in availability studies, Reliab. Eng. Syst. Saf. 8320 (96).

[13] A. Marson, Modeling with generalized stochastic Petri nets, Wiley, New York, 1995.

[14] S. Swaminathan, The Event Sequence Diagram framework for dynamic probabilistic risk assessment, Reliab. Eng. Syst. Saf. 63 (1999) 224.

[15] S. Swaminathan, Dynamic probabilistic risk assessment using event sequence diagrams, Ph.D. thesis, University of Maryland, College Park (1999).

[16] G. A. P. Castaneda, J.-F. Aubry, N. Brinzel, Stochastic hybrid automata model for dynamic reliability assessment, in: IMechE, 2015, pp. 28–41. doi:10.1177/1748006XJRR312.

[17] G. Babykina, N. Brînzei, J.-F. Aubry, G. Deleuze, Modeling and simulation of a controlled steam generator in the context of dynamic reliability using a Stochastic Hybrid Automaton, Reliab. Eng. Syst. Saf. 115–136doi:10.1016/j.ress.2016.03.009.

[18] F. Chiacchio, D. D. Urso, L. Compagno, M. Pennisi, F. Pappalardo, G. Manno, SHyFTA , a Stochastic Hybrid Fault Tree Automaton for the modelling and simulation of dynamic reliability problems, Expert Syst. Appl. 42–57doi:10.1016/j.eswa.2015.10.046.

[19] T. Matsuoka, M. Kobayashi, GO-FLOW: A New Reliability Analysis Methodology, Nucl. Sci. Eng. 98 (1988) 64–78.

[20] J. Zhu, M. Collette, A dynamic discretization method for reliability inference in Dynamic Bayesian Networks, Reliab. Eng. Syst. Saf. 138 (2015) 242–252. doi:10.1016/j.ress.2015.01.017.

[21] P. Weber, L. Jouffe, Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN), Reliab. Eng. Syst. Saf. 91 (2) (2006) 149–162. doi:10.1016/j.ress.2005.03.006.

[22] A. Ben Salem, A. Muller, P. Weber, Dynamic Bayesian Networks in system reliability analysis, in: 6th IFAC Symp. Fault Detect. Superv. Saf. Tech. Process., pp. 481–486. doi:10.1016/B978-008044485-7/50075-0.

[23] S. Montani, L. Portinale, A. Bobbio, D. Codetta-Raiteri, Radyban: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks, Reliab. Eng. Syst. Saf. 93 (7) (2008) 922–932. doi:10.1016/j.ress.2007.03.013.

[24] E. E. Lewis, F. Boehm, Monte Carlo simulation of Markov Unreliability Models, Nucl. Eng. Des. 77 (1984) 49–62.

[25] N. Siu, Risk assessment for dynamic systems: An overview, Reliab. Eng. Syst. Saf. 43 (1) (1994) 43–73. doi:10.1016/0951-8320(94)90095-7.

[26] D. L. Deoss, N. O. Siu, A simulation model for dynamic system availability analysis, Tech. rep. (1989).

[27] C. Smidts, J. Devooght, Probabilistic Reactor Dynamics II : A Monte Carlo Study of a Fast Reactor Transient, Nucl. Sci. Eng. 111 (1992) 241–256.

[28] J. Devooght, Dynamic reliability, Adv. Nucl. Sci. Technol. 25 (1997).

[29] P. E. Labeau, C. Smidts, S. Swaminathan, Dynamic reliability : towards an integrated platform for probabilistic risk assessment, Reliab. Eng. Syst. Saf. 68 (2000) 219–254.

[30] T. Aldemir, A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants, Ann. Nucl. Energy 113–124doi:10.1016/j.anucene.2012.08.001.

[31] J. Devooght, C. Smidts, Probabilistic Reactor Dynamics I : The Theory of Continuous Event Trees, Nucl. Sci. Eng. 240 (1992) 229–240.

[32] J. Vaurio, On time-dependent availability and maintenance optimization of standby units under various maintenance policies, Reliab. Eng. Syst. Saf. (1) 79–89. doi:10.1016/S0951-8320(96)00132-9.