A Benchmark of Dynamic Reliability Methods for Probabilistic Safety Assessment

Xiaolei Pan
College of Automation Engineering,
Shanghai University of Electric Power,
Shanghai, China
e-mail: xiaolei.pan@shiep.edu.cn

Francesco Di Maio, Enrico Zio
Energy Department,
Politecnico di Milano,
Milano, Italy
e-mail: francesco.dimaio@polimi.it, enrico.zio@polimi.it

***Abstract*—Various dynamic reliability methods have been developed during the last several decades, such as Monte Carlo (MC) simulation, Dynamic Event Tree (DET) and Monte Carlo Dynamic Event Tree (MCDET) methods, to name a few. This paper benchmarks these particular methods by applying them to a classic level control dynamic system and to a realistic Emergency and Standby Power System (ESPS). The analysis is done with respect to different component aging dynamics and transition rate state dependences. Efficiency and computational cost are evaluated. The results show that: (1) the dynamic methods indeed are capable of capturing the effects of the dynamics in the process; (2) DET can model the possible accidental sequences, but at a large computational cost; (3) accurate modelling of sequences with low probabilities of occurrence can be achieved by the MCDET method.**

Keywords-Monte Carlo simulation; dynamic event tree; Monte Carlo dynamic event tree; dynamics reliability.

I. INTRODUCTION

Probabilistic Safety Assessment (PSA) is performed by regulatory bodies to check the compliance of nuclear power plant design with regulatory requirements, and by industry for the identification of key vulnerabilities, so that the impact of operational changes on the operating plants can be informed by risk quantification [1-3].

Traditional PSA methods are, for example, Fault Trees (FTs) and Event Trees (ETs), that describe each accident sequence as a combination of success and failure events, accounting for the contribution of each component. Such PSA tools are currently widely used, but some limitations are acknowledged: the conservative assumptions that are made for the sake of PSA modelling simplification may lead to conservative results that, however, still do not assure coverage of the uncertainty therein (e.g. because of imprecise description of component aging and maintenance, binary modelling of components behavior, i.e., only faulty/safe states are considered, and neglecting dynamics of the system, i.e., the effect of order and timing of failure events on the accident progression) [2, 4].

To overcome some of these the limitations, dynamic reliability methods have been developed [5], such as Dynamic Event Tree (DET) [6, 7], the Continuous Cell-to-Cell-Mapping Technique (CCCMT) [8], Monte Carlo (MC) simulation [9], Markov/CCMT [10], Monte Carlo Dynamic Event Tree (MCDET) [11, 12]. The methods of MC, DET and MCDET are the most popular ones.

This paper analyzes critically these latter methods by applying them to a classic level control dynamic system of literature [13-15] and to a realistic Emergency and Standby Power System (ESPS) [16, 17] drawing some conclusions on their strengths (i.e., accuracy) and weaknesses (i.e., computational demand and model complexity) for practical application.

The paper is organized as follows. The methods of MC, DET, MCDET are briefly recalled in Section 2. Section 3 presents and discusses the results of the application of the methods to the level control dynamic system. The ESPS results are presented in Section 4. Finally, conclusions are given in Section 5.

II. THE DYNAMIC RELIABILITY METHODS CONSIDERED

A. Monte Carlo Simulation

Monte Carlo (MC) simulation is a method that allows sampling the events that occur in an accident sequence from given probability distributions. For this, the MC simulation has two loops. The outer loop is iterated a number N of times equal to the number N of sequences to be simulated. This loop also allows for sampling values of process variables affected by epistemic uncertainty [13]. The inner loop allows sampling values of variables affected by aleatory uncertainty and simulates the occurrence of events along the sequence, up to the Mission Time T_M [13]. A flowchart of the inner loop of a MC simulation is shown in Fig. 1.

Statistics of the N sequences simulated by MC, like the Failure Frequency (FF), Mean Time To Failure (MTTF), Mean Time To Repair (MTTF), Sensitivity Indexes (SI) can be estimated.

B. Dynamic Event Tree

A Dynamic Event Tree (DET) has a similar structure to its static counterpart, i.e. the ET, except that, in DET analysis, time is explicitly modelled so that the dynamic evolution of accidental sequences is modelled in a phenomenologically consistent manner [18]. A DET starts from an Initiating Event (IE) on the time axis and simulates the possible sequences which can develop from this IE, by branching at time points of the source branch of the tree. This allows for a wider and faster exploration of the failure domain of the system by simultaneously accounting for more than one sequence of events (contrary to what is done by MC simulation). There are two key issues to be addressed in DET construction: the selection of branching and stopping rules. The following rules are usually used in DET

978-1-5386-3322-9/17/$31.00 ©2017 IEEE

construction: (1) new branches are originated at discrete time points if the probability of the system to stay in the original state (i.e. to continue on the source branch) is smaller than a pre-defined branching probability threshold; (2) only one component can fail at each branching node; (3) when the generated branch probability is smaller than a pre-defined value, the generated branch is truncated and, thus, neglected in the following analysis. A flowchart of DET is shown in Fig. 2.

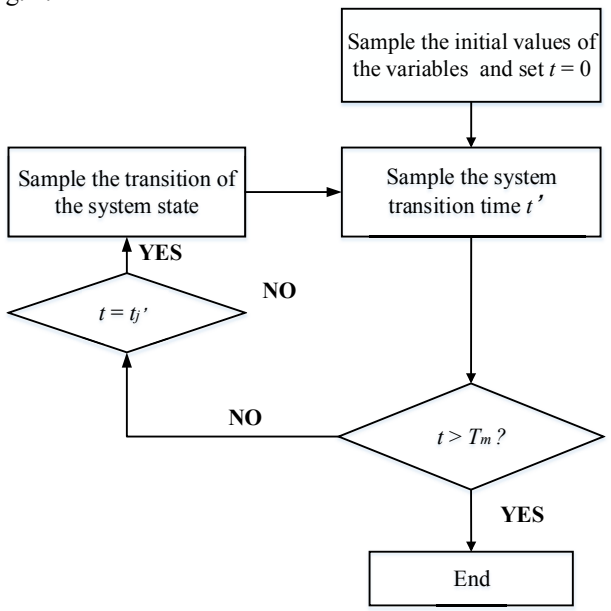

Figure 1. The flowchart of the inner loop of MC simulation

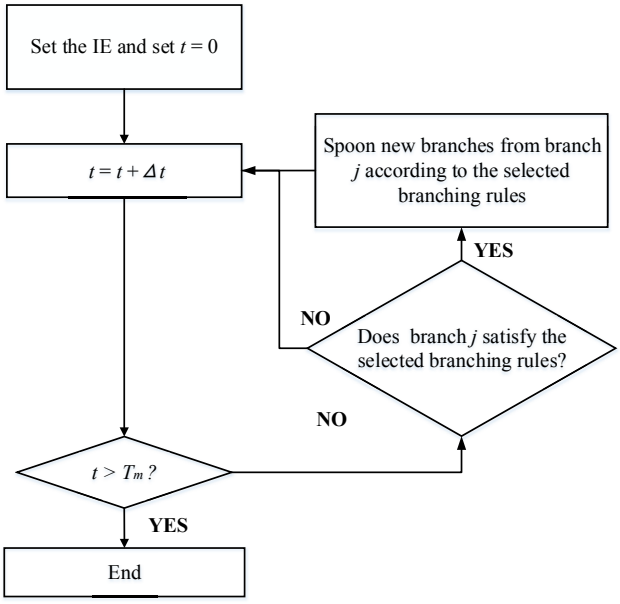

Figure 2. The flowchart of DET

C. Monte Carlo Dynamic Event Tree

Monte Carlo Dynamic Event Tree (MCDET) is a method that combines MC sampling and DET [19]. It is aimed at achieving an even more realistic modelling of system dynamics in the framework of probabilistic safety analyses. In MCDET models, continuous and random uncertainties are handled by MC simulation, while discrete and random uncertainties are treated by DET [11]. Like MC simulation, MCDET has two loops. The outer loop is iterated a number N of times equal to the number N of DETs to be simulated. In the inner loop, each DET starts from an IE and branches at time points along time t, up to the Mission Time T_M, that are sampled according to the MC simulation. As in MC simulation, epistemic uncertainties can also be considered by sampling from their probability distributions in the outer loop. A flowchart of the inner loop of a MCDET is shown in Fig. 3.

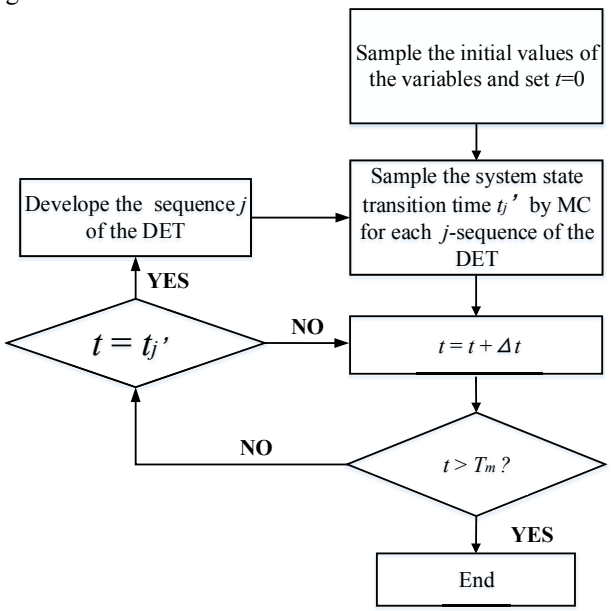

Figure 3. The flowchart of the inner loop of MCDET

III. Case Study 1: The Level Control Dynamic System

A. Description of the System

The system consists of two pumps and one valve that function so as to keep the fluid level of the tank within the interval [6, 8] m by a control system, as shown in Fig. 3. The scope is to keep the tank filled at a constant level h equal to 7 m, by injecting and discharging water at a rate Q equal to 0.6 m/h for pump 1 and the valve, respectively. In normal condition, pump 2 is in standby mode. In case the fluid exceeds any of the two thresholds of 6 m or 8 m, the components states are changed by the control system as shown in Table I, where the rules to keep the level under control are listed. If some components are failed, some transitions might not be allowed and the control of the level might be lost, because the fluid might reach either "*dry-out*" level of 4 m or "*over-flow*" level of 10 m. All the components can work in 4 possible states: *safe-on* and *safe-off* (i.e., normal condition), and *stuck-on* and *stuck-off* (i.e., failed condition). Different kinds of transition rates can be considered for describing the probabilities of transitions of these components among the possible states: constant and

independent on the system state (Table II) or increasing with time and dependent on the system state (Table III). These assumptions lead to considering different probabilistic models: static reliability methods in the former case, dynamic methods (MC, DET and MCDET) in the latter cases.

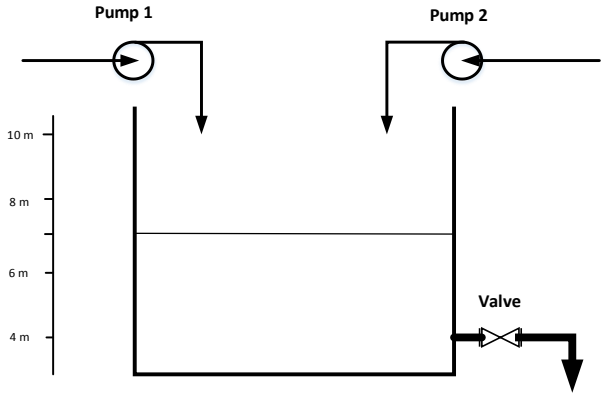

Figure 4. Diagram of the level control dynamic system

TABLE I. CONTROL RULES OF THE LEVEL CONTROL DYNAMIC SYSTEM

	Pump 1	Pump 2	Valve
Fuild level > 8 m	Off	Off	On
Fuild level < 6 m	On	On	Off

TABLE II. FAILURE RATES FOR THE STATIC PSA ANALYSIS

	λ_{on}	λ_{off}
Pump 1	4.566 e-3	4.566 e-3
Pump 2	5.714 e-3	5.714 e-3
Valve	3.125 e-3	3.125 e-3

B. Static PSA Analysis

The failure rate λ of each component of the system is considered to be constant and independent on the system state, $\lambda = \lambda_{on} = \lambda_{off}$ (See (Table II). Moreover, the probability that a component fails *stuck-on*/ *stuck-off* before time *t* is assumed equal to:

$$p_{stuck-on}(t) = p_{stuck-off}(t) = \frac{1}{2}\,[1 - exp(-\lambda t)] \quad (1)$$

The reliability of each component at time *t* is assumed equal to:

$$R(t) = exp(-\lambda t) \quad (2)$$

The probability of the top event ("*over-flow*" and "*dry-out*"), under the rare event approximation, equals to:

$$F(t) = \sum_{r=1}^{m} \prod_{x_b \,\epsilon E_r} q_b(t) \quad (3)$$

where:

m is the number of Minimal Cut Sets (MCSs) causing the top event ("*over-flow*" and "*dry-out*");

E_r is the r^{th} MCS causing the top event;

x_b is the b^{th} basic event in the r^{th} MCS E_r;

$q_b(t)$ is the probability of occurrence of the basic event x_b before time *t*.

Table III lists the m = 6 MCSs for the "*over-flow*" and "*dry-out*" top events. The probabilities of the top events to occur within T_m = 30 h are 0.0110 and 0.000226 respectively, and 0.4080 and 0.0836 for T_m = 500 h. The plots of F(t) are shown in Fig. 5.

TABLE III. MINIMAL CUT SETS OF THE FAILURE OF THE LEVEL CONTROL DYNAMIC SYSTEM [15]

Top event	Minimal Cut Sets (MCSs)
"*over-flow*" (5 MCSs)	$Pump1_{stuck\,on}$, $Pump2_{stuck\,off}$, $Valve_{stuck\,off}$
	$Pump1_{stuck\,off}$ $Pump2_{stuck\,on}$, $Valve_{stuck\,off}$
	$Pump1_{safe}$, $Pump2_{stuck\,on}$, $Valve_{stuck\,off}$
	$Pump1_{stuck\,on}$, $Pump2_{safe}$, $Valve_{stuck\,off}$
	$Pump1_{stuck\,on}$, $Pump2_{stuck\,on}$
"*dry-out*" (1 MCS)	$Pump1_{stuck\,off}$, $Pump2_{stuck\,off}$, $Valve_{stuck\,on}$

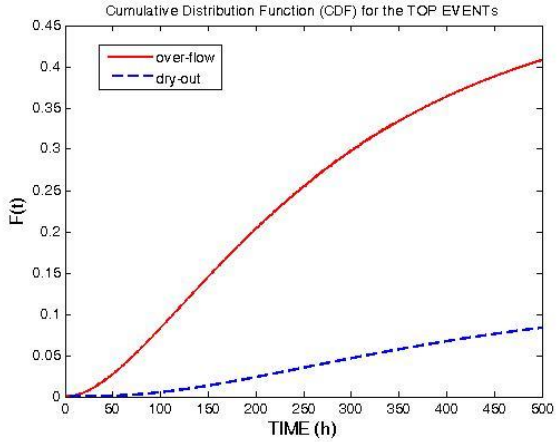

Figure 5. Cumulative Distribution Function (CDF) for the top events "*over-flow*" and "*dry-out*"

C. Dynamic PSA Analysis

The demand of reality in modeling the behavior of components and systems calls for transition rates that account for aging (i.e., they increase with time) and that depend on the system state. For the impact of aging on the transition rates, we assume the following linear form [20]:

$$\lambda(t) = \lambda_0 + kt \quad (4)$$

where:

$\lambda(t)$ is the transition rate at time *t*,

λ_0 is the design transition rate, (i.e. the value at time *t* = 0),

k is the aging factor

The transition rates dependences on the system state are given in Table IV.

Under these circumstances, we adopt dynamic methods for reliability modelling. To benchmark the different

methods and compare with the static method of section 3.2, four different cases are considered:

1) no aging and no transition rates dependence on the system state
2) slow aging and no transition rates dependence on the system state
3) fast aging and no transition rates dependence on the system state
4) no aging and transition rates dependence on the system state

Control rules of the level control dynamic system listed in Table I hold for all the four above mentioned cases. For each case, MC, DET and MCDET models are constructed for T_m = 30 h. The time step Δt considered is set equal to 0.1 h for MC and MCDET, whereas for the DET model, is set equal to 0.66 h. The DET branching probability threshold and truncation probability threshold, aimed at reducing the branching explosion, are set equal to 0.999 and 1×10^{-9} (i.e., branches with lower probability are neglected), respectively.

All the dynamic models have been run on a single node of the super-computing center of the University of Science and Technology of China (USTC) (Intel Xeon E5620, 4 CPU, 2.4GHz, 16GB)

TABLE IV. TRANSITION RATES THAT DEPEND ON THE SYSTEM STATE

	$\lambda_{safe-off \rightarrow stuck-off}$	$\lambda_{safe-off \rightarrow stuck-on}$	$\lambda_{safe-on \rightarrow stuck-off}$	$\lambda_{safe-on \rightarrow stuck-on}$
Pump 1	4.566 e-1	4.566 e-2	4.566 e-3	4.566 e-3
Pump 2	5.714 e-3	5.714 e-3	5.714 e-1	5.714 e-2
Valve	3.125 e-1	3.125 e-2	3.125 e-3	3.125 e-3

D. Results and Discussions

In Fig. 6, the plots of F(t) obtained with the static PSA analysis of Section 3.2 (continuous line) are compared with those of the dynamic PSA analysis of Section 3.3 (crosses, left and right triangles for DET, MC and MCDET, respectively), for the case of no aging and no transition rates dependence on the system state. It can be seen that the static PSA model overestimates both failure modes with respect to the dynamic models, at any time. This is mainly due to the assumption made with the static modelling, for which the system fails as soon as any of its MCS occurs; however, the real dynamics of the system does not imply the sudden system failure when a MCS occurs. For example if one pump fails *stuck-on* and the valve *stuck-off* at any time *t*, the system exceeds the level thresholds only several hours later due to the actual discharging/injecting rate Q of the pumps and valve, that is, instead, neglected in the static PSA model.

On one hand, such assumption in static PSA causes the probabilities of the top events to be greater than the actual ones. On the other hand, the capability of dynamic probabilistic methods to properly account for the dynamics into the quantification become evident.

Focusing on the dynamic methods, Fig. 6 (right) shows that the estimate provided by the MCDET is smoother than that provided by the MC simulation, because the former (by exploring simultaneously more than one branch of the possible developing scenarios) allows collecting more evidence of system failure than the latter with the same computational effort (as we shall see in what follows).

The capability of dynamic methods to catch the aging effects is shown in Fig. 7 and Fig. 8 for T_m= 30 h and T_m= 500 h, respectively. It can be seen that, at the early stage of the system life, the impact of the components aging on the result is negligible (crosses, left and right triangles are almost overlapped), because the change of the transition rates caused by the aging factors is limited (see Eq (4)). On the other hand, as long as the system degrades, the aging effect is predominant and the transition rates values increase, and the impact becomes considerable already after 100 hours for *k* = 1e-5 (left triangles).

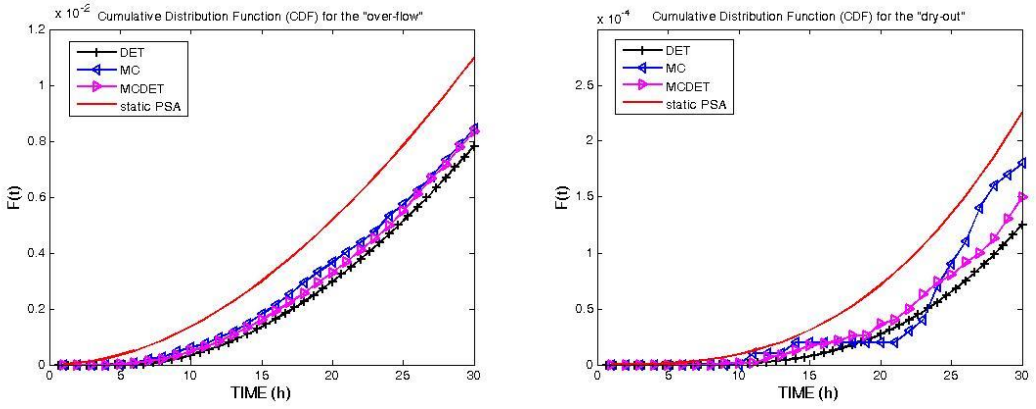

Figure 6. Cumulative Probability Distribution for "over-flow" (left) and "dry-out" (right) with T_m= 30 h and N = 100000, for the case of no aging and no transition rates dependence on the system state

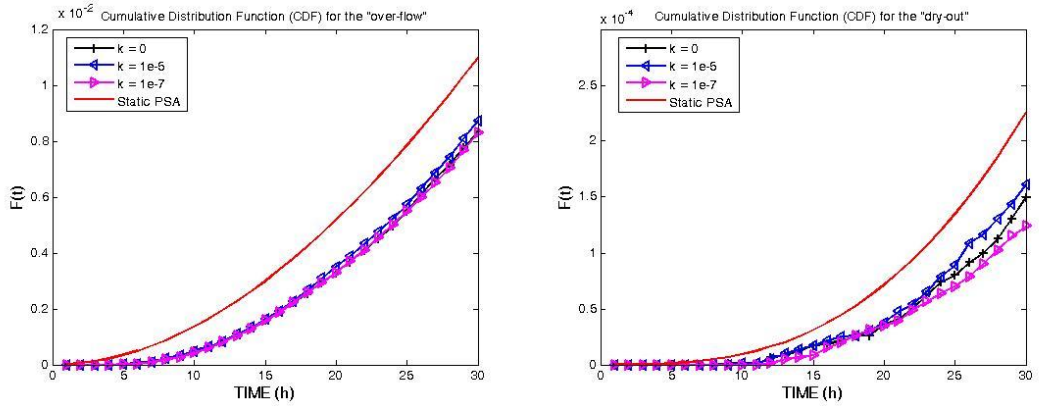

Figure 7. Cumulative Probability Distribution for "over-flow" (left) and "dry-out" (right) with T_m= 30 h and N = 100000, for the case of aging and no transition rates dependence on the system state

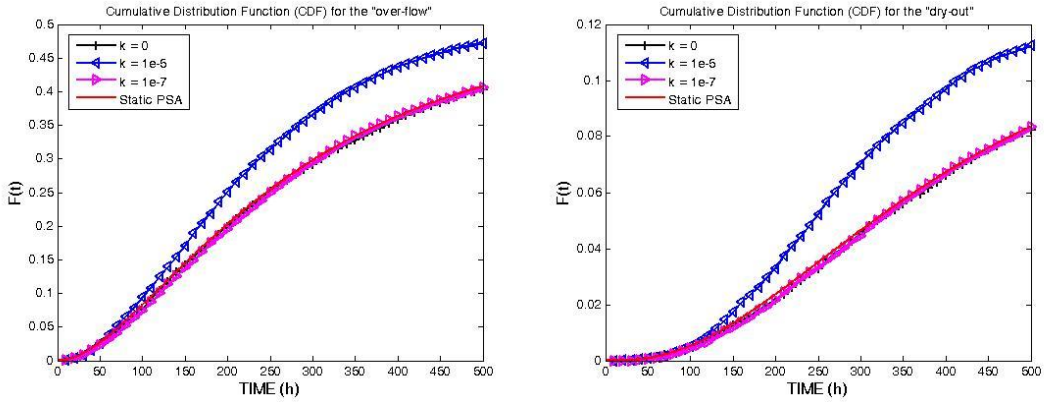

Figure 8. Cumulative Probability Distribution for "over-flow" (left) and "dry-out" (right) with T_m= 500 h and N = 10000, for the case of aging and no transition rates dependence on the system state

The capability of dynamic methods to catch the dependence of the components transition rates on the system state (Table III and case 4) is shown in Fig. 9 and Fig. 10. It can be seen that the probability of the system failure in the early stage is much larger than the ones shown in Fig. 6, especially for the probabilities of "*dry-out*". It is worthy to note that as long as time increases, the "*over-flow*" and "*dry-out*" probabilities reach the estimated values of Fig. 6 at about 370 h and 470 h, respectively. This is due to the fact that the considered level control system is a non-coherent system. Although transition rates increase with respect to the base case of no aging and no dependence on the system state, the number of component contributions that lead the system into any of the two top failure modes decreases.

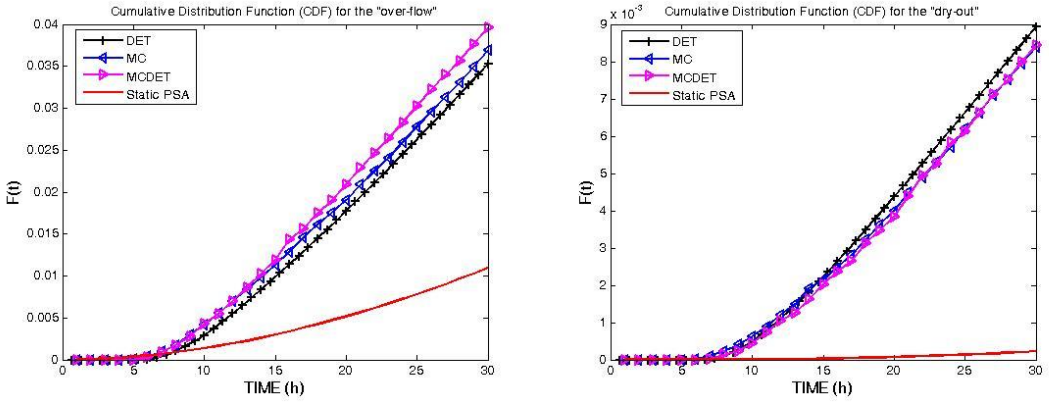

Figure 9. Cumulative Probability Distribution for "over-flow" (left) and "dry-out" (right) with T_m= 30 h and N = 100000, for the case of no aging and transition rates dependence on the system state

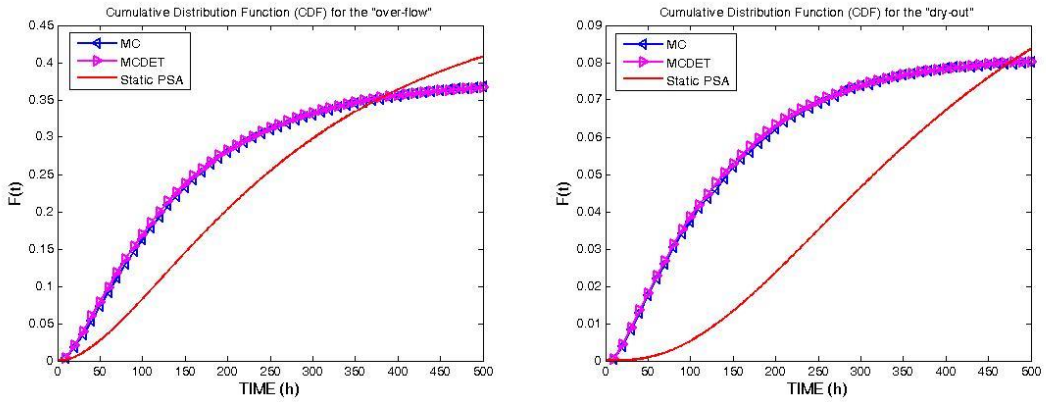

Figure 10. Cumulative Probability Distribution for "over-flow" (left) and "dry-out" (right) with T_m= 500 h and N = 10000, for the case of no aging and transition rates dependence on the system state

TABLE V. COMPUTATIONAL EFFICIENCY FOR DET, MC AND MCDET MODELS

Case	Model	Number of Cycles, *N*	Computational cost [s]	Number of "*over-flow*"	Number of "*dry-out*"	Expected time to "*over-flow*" [s]	Expected time to "*dry-out*" [s]
Case 1	DET (T_m=30 h)	-	16004	157784	52914	-	-
	MC (T_m=30 h)	300000	656272	2643	36	248	18229
	MCDET (T_m=30 h)	100000	219123	3496	124	63	1767
	MC (T_m=500)	10000	30668	3996	826	7.67	37.13
	MCDET (T_m=500)	3000	14606	6851	1977	2.13	7.39
Case 2	DET (T_m=30 h)	-	9669	157784	52914	-	-
	MC (T_m=30 h)	300000	638364	2494	39	256	16368
	MCDET (T_m=30 h)	100000	241849	3479	100	70	2419
	MC (T_m=500)	10000	21322	4124	790	5.17	26.99
	MCDET (T_m=500)	3000	14410	6892	1999	2.09	7.21
Case 3	DET (T_m=30 h)	-	9524	157784	52914	-	-
	MC (T_m=30 h)	300000	657328	2701	39	243	16855
	MCDET (T_m=30 h)	100000	246248	3707	131	66	1880
	MC (T_m=500)	10000	34685	4745	1099	7.31	31.56
	MCDET (T_m=500)	3000	16208	8414	2697	1.93	6.01
Case 4	DET (T_m=30 h)	-	8523	127482	45554	-	-
	MC (T_m=30 h)	300000	308595	3729	929	83	332
	MCDET (T_m=30 h)	20000	33189	10795	3333	3.07	9.99
	MC (T_m=500)	30000	71527	11014	2024	6.49	29.75
	MCDET (T_m=500)	10000	42566	2956	9856	1.51	4.59

Although dynamic methods (MC, DET and MCDET) have shown superior capabilities with respect to static PSA methods, the computational cost may be large. The computational cost, indeed, depends on the length of the discrete time step that is simulated, the length of the mission time T_m to be simulated, the branching probability thresholds that is set (only for DET) and the selected number of repeated sampling cycles *N* (only for MC and MCDET). Fig. 11 shows the computational costs of the MC, DET and MCDET models for the base case of no aging and no

transition rates dependence on the system state as a function of T_m. The computational cost of DET model increases exponentially as the T_m increases, while the computational costs of MC and MCDET models increase approximately linearly with T_m. So DET model is only applicable when a limited T_m is foreseen to be modelled. For long T_m, MC and MCDET models seem more appropriate than DET.

A more detailed analysis and comparison among DET, MC and MCDET is presented in Table V, that lists the computational efficiency of the selected dynamic methods when applied to the four cases 1), 2), 3) and 4) illustrated in section 3.3. For the purpose of comparison, we define computational efficiency as the capability of a method to collect evidences of system failure (i.e., number of "*over-flow*" and "*dry-out*") with a given computational effort (i.e., number of MC cycles (*N*), computational cost [s], expected time to "*over-flow*" [s] and to "*dry-out*" [s]). The results show that the MCDET method is much more effective to collect the evidences of "*over-flow*" and "*dry-out*" than MC simulation at same T_m, because the sequences with low probability of occurrence are not discarded. For example, when no aging and no dependence of the transition rates on the system state (case 1) is simulated and T_m is equal to 30 h, the expected times for simulating one "*over-flow*" with MC and MCDET are 248 s and 63 s, respectively, and the expected times to "dry-out" are 18229 s and 1767 s, respectively.

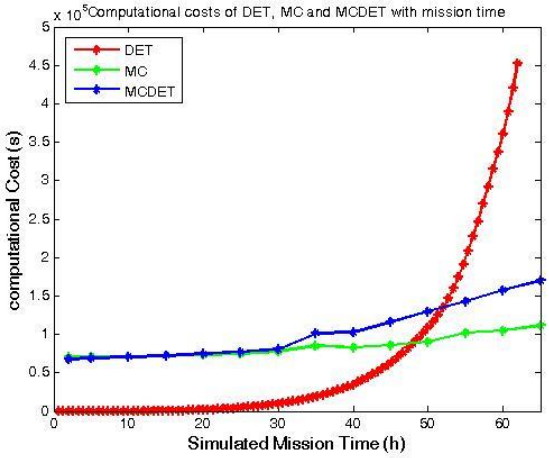

Figure 11. Computational cost of DET, MC and MCDET as a function of the mission time T_m

IV. Case Study 2: The Emergency and Standby Power System (ESPS)

A. Description of the System

Emergency and standby power systems (ESPS) are designed to provide a plant alternative source of power when the normal source of power, the Utility Input Power (UIP), fails. A sketch of the system is shown in Fig. 12 [16, 17]. The power is normally supplied by the UIP while two generators (G1 and G2) are kept in cold standby mode, with probability of failure on demand p_s equal to 0.015. A synchronized bypass and a static transfer switch (STS) protect the critical load in the event of inverter failure. If voltage is lost at the Critical Load Bus (CLB), STS reestablishes voltage in less than one-quarter of a cycle. If the power fails at bus A, the battery can supply the power for 4 h.

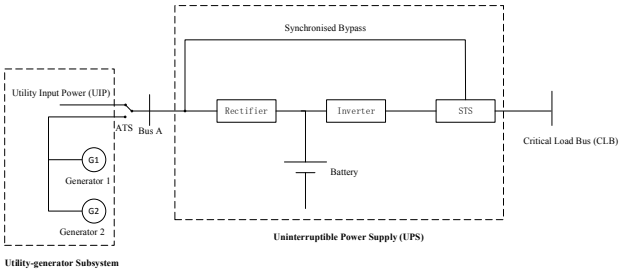

Figure 12. Diagram of Emergency and Standby Power Systems

Table VI shows the reliability data for all the components of the ESPS system that are considered repairable. It is important to notice that only one generator can be taken out for maintenance and that if a generator fails while another is on maintenance, the maintenance on the second generator would be accelerated by a factor of α, setting $\alpha = 2$ in this case. The fault tree for the top event "power loss at the Critical Load Bus (CLB)" is shown in Fig. 13.

TABLE VI. Reliability Data for Various Components of the ESPS System

Equipment/Supply	λ (f/y)	R (h/f)
Utility Input Power	0.53700	5.66
Generator (G1/G2) (per hour of use)	0.00536	478.00
Inverter	1.25400	107.00
Rectifier	0.03800	39.00
Automatic Transfer Switch (ATS)	0.00600	5.00
Static Transfer Switch (STS)	0.08760	24.00
Battery	0.03130	24.00
Equipment Maintenance	**Frequency (/y)**	**Duration (h)**
Generator (G1/G2)	1.00	10.00
Uninterruptible Power Supply (UPS)	1.00	4.00

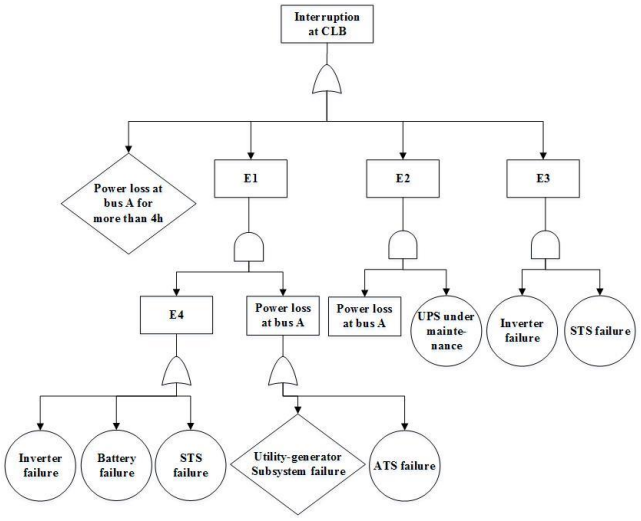

Figure 13. Fault tree of "power loss at the Critical Load Bus (CLB)"

The reliability analysis of the ESPS system is made by the MC method, the Markov method and minimal cut set

method, respectively in reference [16] and [17]. In this work, we benchmark the results with those that we obtain with MC and MCDET models.

B. Dynamic PSA Analysis

MC and MCDET models are built for the reliability analysis of the ESPS system. These would allow considering the dependencies between components (i.e., accidental maintenance on generators, when at least one of the two is out of order). The time discretization considered for the simulation is set equal to 0.1 h. The only difference between the two models is that only one sequence of events can be simulated with one cycle of MC model, whereas for MCDET, that same sequence of event may branch out into several branches at the selected branching nodes of the DET. Two models are run on the single node of the super-computing center of USTC (Intel Xeon E5620, 4 CPU, 2.4GHz, 16GB).

C. Results and Discussions

MC and MCDET models are used to compute the reliability parameters for the ESPS (listed in Table VII) to be compared with those obtained with Markov methods [17]: frequency (f_p) and duration (r_p) of failure of the utility-generator subsystem, frequency (f_A) and duration (r_A) of power loss at bus A, and frequency (f_{CLB}) and duration (r_{CLB}) of power loss at CLB estimated confidence intervals (i.e., estimated values ± standard deviation) are all bounding the values calculated in [17], confirming the capability of MC and MCDET of effectively modelling the system dynamics.

The computational efficiency in capturing the evidence of failure for each developed dynamic model is shown in Table VIII. The same conclusion of Section 3.4 can be drawn from this case study: the MCDET method is more effective to collect evidences of failure with respect to MC simulation. For example, the MC model with 50000 cycles models cut-set E1 three times whereas cut-set E2 is modelled zero times within mission time $T_m = 1\ y$, while the MCDET model, with the same number of cycles and T_m, models cut-set E1 42 times and cut-set E2 only 2 times. The probability distributions of duration of power loss at the CLB obtained by the two dynamic models are displayed in Fig. 14.

TABLE VII. RELIABILITY PARAMETERS OBTAINED FROM MC AND MCDET MODELS

	Estimated value in [17]	**MC (50000 cycles)**		**MCDET 50000 cycles)**	
		Estimated value	***Confidence interval*** *[Estimated value ± standard deviation]*	***Estimated value***	***Confidence interval*** *[Estimated value ± standard deviation]*
f_p	0.00157	0.00184	[0.00152, 0.00216]	0.00184	[0.00158, 0.00211]
r_p	5.4532	5.5152	[4.5038, 6.5266]	5.5072	[5.3368, 5.6776]
f_A	0.00757	0.00798	[0.00733, 0.00863]	0.00781	[0.00718, 0.00843]
r_A	5.0938	5.0005	[4.9656, 5.0354]	5.3407	[5.1873, 5.4941]
f_{CLB}	0.00523	0.00540	[0.00486, 0.00594]	0.00593	[0.00537, 0.00648]
r_{CLB}	9.648	11.5402	[10.3767, 12.7037]	9.4789	[9.1177, 9.8402]

TABLE VIII. STATISTICS OF COMPUTATIONAL EFFICIENCIES OF CAPTURING THE EVIDENCE OF FAILURE FOR EACH MODEL

Events	**MC (50000 cycles)**		**MCDET (50000 cycles)**	
	Number of evidences	*Expected time for capturing an evidence*	*Number of evidences*	*Expected time for capturing an evidence*
Failure of utility-generator subsystem	102	747	2770	73
Failure of ATS	307	248	550	370
Failure of power supply over 4 h	47	1587	1330	153
Failure of ATS over 4 h	141	540	261	780
Cut-set E1	3	25392	42	4845
Cut-set E2	0	-	2	101739
Cut-set E3	78	977	161	1264
Power loss at CLB	276	276	1796	113

V. CONCLUSION

This paper analyzes dynamic methods for PSA by application to two systems. The methods considered (MC, DET and MCDET) are shown to overcome the classic PSA methods (FT/ET), for systems where dynamic factors like aging and dependence among components play a significant role. They, indeed, allow accounting for the variation of failure rates depending on system state, and the order and timing of failure events along an accidental scenario. As a

matter of fact, as shown with respect to the level control system and ESPS system case studies, dynamic methods are more flexible to incorporate various effects of the dynamics of the process, compared with static PSA methods. A comparison of the dynamic PSA methods implemented shows that the computational costs of the DET method are large when long mission times are to be simulated, and that MCDET is more effective to simulate failure sequences of events than MC method with the same computational effort.

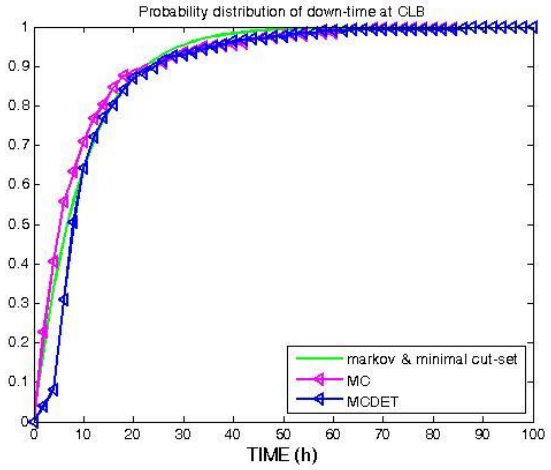

Figure 14. Probability distributions of duration of power loss at the CLB

ACKNOWLEDGEMENT

The numerical calculations in this paper have been done on the supercomputing system in the Supercomputing Center of University of Science and Technology of China. We further thank the great help from other members of LASAR Team in this research.

REFERENCES

[1] IAEA. Applications of probabilistic safety Assessment (PSA) for nuclear power plants. IAEA-TECDOC-1200, 2001.

[2] F. Di Maio, M. Vagnoli, and E. Zio, Transient identification by clustering based on integrated deterministic and probabilistic safety analysis outcomes. Annals of Nuclear Energy, vol. 87, Part 2: pp. 217-227. 2016.

[3] F. Di Maio, P. Secchi, S. Vantini, and 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, Vol. 60 (2), pp. 415-425. June 2011.

[4] F. Di Maio, S. Baronchelli, E. Zio, A computational framework for prime implicants identification in noncoherent dynamic systems. risk analysis. Vol. 35(1): pp. 142-156. 2015.

[5] T. Aldemir, A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Annals of Nuclear Energy. Vol. 52: pp. 113-124. 2013.

[6] E. Hofer, M. Kloos and B. Krzykacz-Hausmann, Dynamic event trees for probabilistic safety analysis. GRS, Garsching, Germany, 2004.

[7] C. Acosta and N.O. Siu, Dynamic event tree analysis method (DETAM) for accident sequence analysis. Massachusetts Institute of Technology, 1991.

[8] B. Tombuyses and T. Aldemir, Continuous cell-to-cell mapping. Journal of sound and Vibration. Vol. 202(3): pp. 395-415. 1997.

[9] E. Zio, The Monte Carlo simulatn method for system reliability and risk analysis. Springer. 2013.

[10] I.B. Gomes, P.F. Melo, and P.L. Saldanha, A cell-to-cell Markovian model for the reliability of a digital control system of a steam generator. UFRJ/COPPE/Programa de Engenharia Nuclear, 2013.

[11] M. Kloos and J. Peschke, MCDET: a probabilistic dynamics method combining monte carlo simulation with the discrete dynamic event tree approach. Nuclear science and engineering. Vol. 153(2): pp. 137-156. 2006.

[12] M. Sonnenkalb, J. Peschke and M. Kloos, MCDET and MELCOR–an example of a stochastic module coupled with an integral code for PSA Level 2. International Workshop on Level 2 PSA and Severe Accident Management. Köln, Germany. 2004.

[13] D.R. Karanki, V.N. Dang, and M.T. MacMillan, Uncertainty propagation in dynamic event trees - initial results for a modified tank problem. Probabilistic Safety Assessment and Management PSAM 12, Honolulu, Hawaii. 2014.

[14] F. Di Maio, M. Stasi and E. Zio, Identification of faults in a level control dynamic system. ANS NPIC HMIT 2009 Topical Meeting - Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology, Knoxville, Tennessee. pp. 1228-1239. 2009.

[15] M. Marseguerra and E. Zio, Monte Carlo approach to PSA for dynamic process systems. Reliability Engineering and System safety. Vol. 52. pp. 227-241. 1996.

[16] C. Singh and J. Mitra, Monte Carlo simulation for reliability analysis of emergency and standby power systems. In Industry Applications Conference. Vol. 3. Pp. 2290-2295. 1995,

[17] C. Singh, N. Gubbala, and N. Gubbala, Reliability analysis of electric supply including standby generators and an uninterruptible power supply system. IEEE transactions on industry applications. 130(5): pp. 1298-1302. 994.

[18] Nuclear Regulatory Commission. Severe accident risks: an assessment for five US nuclear power plants. No. NUREG--1150-vol. 3. Nuclear Regulatory Commission, 1991..

[19] E. Hofer, M. Kloos, and B. Krzykacz. Methodenentwicklung zur simulativen Behandlung der Stochastik in probabilistischen Sicherheitsanalysen der Stufe 2. Garching: GRS-A-2997, Gesellschaft für Anlagen-und Reaktorsicherheit, Germany.2001.

[20] D. Kančev and M. Čepin. Ageing within PSA: development of an analytical unavailability model and its application. European Nuclear Young Generation Forum, Prague. 2011.