A Repairable Dynamic Event Tree Framework for the Safety Assessment of a Steam Generator of a Nuclear Power Plant

Francesco Di Maio [1*], Claudia Picoco [1], and Enrico Zio [1,2]

[1]*Energy Department, Politecnico di Milano, Via La Masa 34, 20156 Milano, Italy*
francesco.dimaio@polimi.it; enrico.zio@polimi.it
Chair System Science and the Energy Challenge, Fondation Electricité de France (EDF), CentraleSupélec, Université Paris Saclay, 92290 Paris, France
enrico.zio@supelec.fr; enrico.zio@edf.fr

Traditional Deterministic Safety Assessment (DSA) and Probabilistic Safety Assessment (PSA) of complex systems have been recently challenged by the excessive conservatism of DSA and the demanding treatment of uncertainties of PSA. In order to deal with these challenges, new methodologies have been developed which result from the integration of DSA and PSA methods for an Integrated Deterministic and Probabilistic Safety Analysis (IDPSA). In this work, we show the capabilities of a Repairable Dynamic Event Tree (RDET) who sets its basis on the traditional static Event Tree (ET) while focusing on the dynamic aspects of accident scenarios thereby described (e.g. timing and magnitude of occurrence of components failure events and repair), as an integrated methodology for IDPSA. We apply the framework of the RDET for the reliability assessment of a U–Tube Steam Generator (UTSG), in which we assume that four components can fail (with different timing and magnitude of failure) and can be repaired. The results of the RDET are benchmarked with those of a traditional ET and of a Repairable ET (RET).

Keywords: Repairable Dynamic Event Tree, Dynamic PSA.

I. INTRODUCTION

The Deterministic Safety Assessment (DSA) for a Nuclear Power Plant (NPP) aims at predicting the response of the NPP to a postulated limited number of Initiating Events (IE) for demonstrating, by adopting conservative assumptions in the physical modelling of the occurring phenomena to "cover" all the phenomenological uncertainties, that the consequences of the postulated Design Basis Accidents (DBAs) are acceptable for both the public and the environment[1].

The Probabilistic Safety Assessment (PSA) not only considers DBAs with more realistic and less conservative hypotheses, but also Beyond Design Basis Accidents (BDBAs) for extending the consequences analysis to a wider set of possible accidental scenario with respect to DSA[2].

PSA is challenged by the lack of data to be used for the scenarios probability quantification and to the static characteristics of Event Trees (ETs) and Fault Trees (FTs) that are typically used for PSA, despite their limits in treating components interactions and dependences, components failure and repair, control and the operator actions, software and firmware failures[3].

Integrated Deterministic Probabilistic Safety Assessment (IDPSA) is a collective name for the variety of different tools which use tightly coupled deterministic and probabilistic approaches to address in a consistent manner aleatory (stochastic aspects of scenario) and epistemic (modelling) uncertainties[3]. IDPSA (also called dynamic reliability) leads to some important advantages with respect to DSA/PSA such as:

- the resolution of time-dependent interactions between physical phenomena, equipment failures, safety and non-safety systems, control logic and operator actions (with Monte Carlo Dynamic Event Tree[4–6], DYnamic Logical Analytical Methodology[7–9], Dynamic Discrete Event Tree[10], Dynamic Event Tree Analysis Method[11], Integrated Safety Assessment[12])
- the identification of a-priori unknown vulnerable scenarios and to reduce the reliance on expert judgment (see[13–15]).

These dynamic methodologies have been, thus, introduced to allow considering the sequence of events (in terms of order, timing and magnitude of failures in the safety analysis) which naturally come from the evolution of the system and cannot, therefore, be predefined by the analyst as in the classical DSA/PSA methods. From this point of view, a more realistic analysis needs to take into account not only timing, order and magnitude of the different failure events but also the possibility of repair of the different failed components. The repair can either restore the system into a safe scenario or, if the system is non –

coherent[14], to more hazardous scenarios, such as Near Misses (NMs) and Prime Implicants (PIs)[14,16] that might endanger the operational state of the plant.

In this work, we analyze the advantages of a Repairable Dynamic Event Tree (RDET) in comparison with a static Event Tree (ET) and a Repairable Event Tree (RET) for calculating the reliability of a system, accounting also for PIs and Near Misses that would be, otherwise, neglected.

The system here analyzed is a U–Tube Steam Generator (UTSG) of a NPP. In this system, we consider that four components can fail: the outlet steam valve, the PID controller, the communication between the level sensor and the controller, and the safety relief valve. The static reliability analysis at the basis of the ET considers binary states for the components, whereas in the dynamic analysis at the basis of the DET the complexity of the components behaviors leads us to adopt a Multiple-Value Logic (MVL) representation of the discretized timing and the magnitude of component failures[17,18]. Therefore, MVL theory gives us the possibility to increase the limited description capability of binary variables in modeling the different component operational states[18]. Thank to this approximation we can realistically analyze the system that, otherwise, would have been computationally intractable[16].

The paper is organized as follows. In Section 2, a survey on the Repairable Dynamic Event Tree (RDET) methodology is given together with the benefits it is expected to show with respect to a static ET, a RET and a DET. Section 3, the model of the UTSG used to generate the scenarios for the reliability analysis is presented and results are shown. Then, conclusion are drawn.

II. THE REPAIRABLE DYNAMIC EVENT TREE

Dynamic methodologies are defined as those that use a time–dependent phenomenological model of system evolution along with its stochastic behavior to account for possible dependencies between failure events[2].

In particular, the DET methodology is (in principle) similar to a static ET (where the sequence of system responses following an IE is predetermined by the analyst) except that both the timing and sequence of system responses are determined by a time-dependent model of system evolution and branching conditions by a probabilistic model of event occurrence[2]. The time-dependent model of the systems allows for a multivalued description of components states which, therefore, accounts for different timing, order and magnitude of the possible failure events, leading, consequently, to a multitude of possible scenarios much larger than in a classical PSA analysis where components states are defined by a binary reasoning (i.e., failed or not failed).

In this way, with a DET, we can fully account for a time-dependent reliability assessment that considers the interactions between system dynamics and stochasticity of events in the evaluation of accident consequences and their conditional probabilities to the IE[6].

In complex systems such as NPPs there are, however, some safety systems for which the possibility of repair has to be foreseen and modeled since maintenance strategies are strictly enforced on these systems to guarantee large availability and reliability targets; typically, these are electrical supply systems, I&C systems and ventilation systems[19].

A modeling effort is due for including into any possible NPP accidental scenario evolution the grace period of components, upon failure. The grace period is, indeed, defined as the time between the failure of the single component and the failure of the system, and it is determined by the physical behavior of the system. The knowledge on the grace period is fundamental to inform the maintainer for accomplishing the repair process within this critical time, and accordingly modifying the design of the system or introducing innovative design[19]. Thus, the safety of such systems can be ensured only if repair of failed components is performed within the grace period[19]. A complete dynamic safety analysis has, thus, to include the possibility of repair during the time evolution of the accidental sequences. This is even more important considering that, due to the non-coherence of some complex systems, it could happen that the repair of some components could also result in unexpected harmful scenarios.

A Repairable Event Tree (RET) (in a classical PSA) is expected to model accident sequences after an IE with the possibility of repairing failed components[19]. In a RET, the accident progression beyond repairable failed branches is virtually ceased if a component i repair time $t_{r,i}$ is less than its grace period $t_{g,i}$. Otherwise, it continues by sequentially following the binary paths of the ET through the remaining branches[19]. In Fig. 1 a RET is shown as an example. In the system considered, four Safety Barriers (SB) work to protect the core after an IE[19]. The possible scenarios are branched depending on the failure of the barriers. Safety barriers 1 and 3 (SB_1 and SB_3) can be repaired after failure. The repair is successful only if their repair times is less than the corresponding grace periods. For SB_2 and SB_4, instead, repair is assumed not to be possible and, thus, their grace periods are set equal to 0. For each scenario, the probability of occurrence can be computed (provided that the branching probabilities are known), resulting in P_1, P_2, P_3, P_4 and P_5.

With respect to a traditional ET, in a RET, success branches probability is given by the probabilities of branches when failure does not occur plus the probabilities of branches whose success is conditioned to the probability the failure occur but the repair time is less than the grace period (and, thus, the repair is successful). On the other hand, in failure branches, the failure probability is given by the failure probability conditioned to the probability that the repair does not occur within the

grace period. Therefore, for each component, with respect a classical ET analysis, failure branches probability is expected to decrease, whereas success branches probabilities is expected to increase due to restoration of components within the grace period, if the system is coherent[16,17]. If the system is not coherent, repairs of components do not imply the restoration of the system into a safe state because, in this latter case, both failed and working states of the same components can lead the system to failure[14].

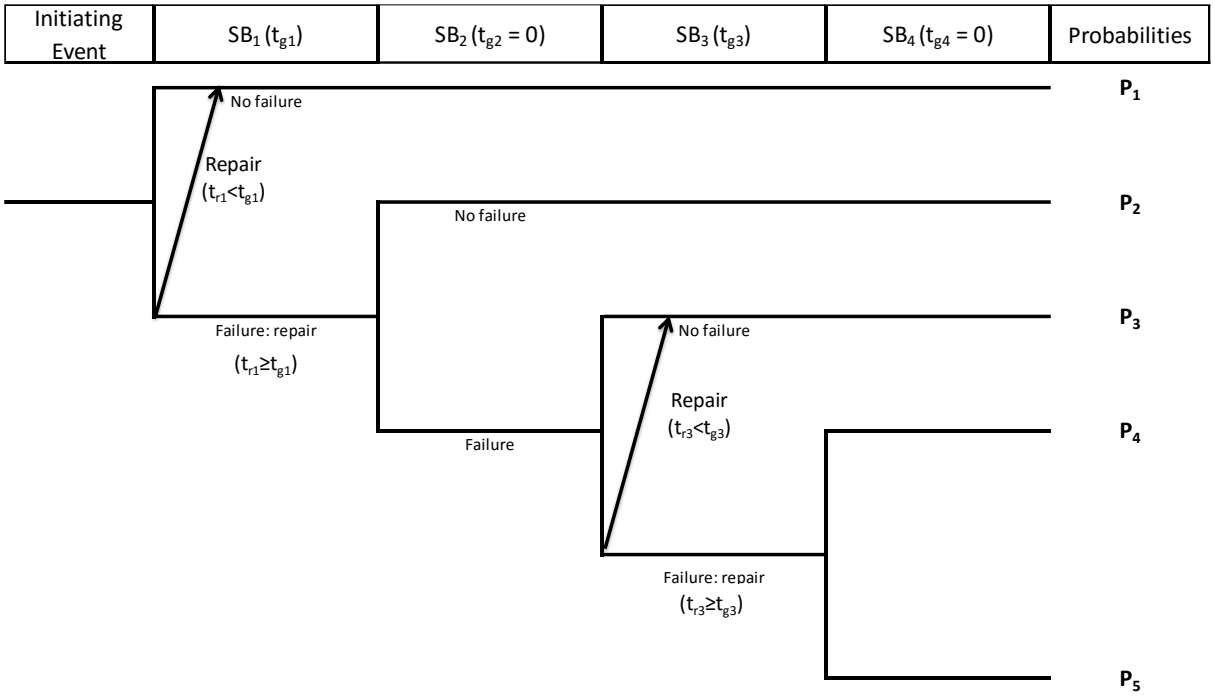

Fig. 1. A RET, adapted from[19].

While a RET provides a framework for including repair events in the modelling of the physical processes behind the system dynamics, a DET analysis provides a framework to simulate the accidental scenarios considering the system dynamic interactions[20]. Both the physical process model, which describes the physical interaction and the time evolution of the system, and the stochastic model, which represents the failure/repair events, are affected by uncertain parameters (such as the time of failure of the different components, the repair time, the magnitude of the failure, and all the boundary and initial conditions which define the phenomena occurring during the accidental scenarios simulation by a thermal–hydraulic (TH) code). All these uncertain variables can significantly affect the simulated accident dynamics and, ultimately, the risk estimates. For this reason, they have to be accounted in the reliability analysis[20]. The proposal of the RDET within an IDPSA is expected to overcome the limits of static approaches to treat these uncertainties, by adding the increased capabilities of scenario exploration of DET to the proper treatment of time-dependencies in components repair processes of a RET[3]. The consistent treatment of uncertainties is guaranteed by the due account of magnitude and time of failure occurrence that are sampled from assumed probability distributions in order to explicitly account for the aleatory uncertainty due to the inherent stochasticity of the failure event as done in DETs (and not in ET, where the analysis is done with fixed times and magnitudes that correspond to the most conservative values) and of repair times that are sampled in an analogous way, from given probability distributions to take into account the randomness of the repair events.

The main benefit of the here proposed RDET framework is that, by taking into consideration as much as possible uncertain scenarios, the binary (failed or safe) consequences modeling of a ET is overcome by the RDET, where, instead, the inherent uncertainty of both failure and repair events does not lead univocally the system to fail or not as we shall see in the next Section.

As last remark it is worth mentioning that when time, magnitude and order of all the possible failures and repair are taken into account, the number of possible combinations increases exponentially and, thus, the identification of the combinations of components failures that are Minimal Cut Sets (MCSs) (i.e., the minimal combination of failure events that leads the system to failure) turns out to be meaningless to describe the system state because, even if the same components fail, their failures times, order, and magnitudes can lead the system into both a safe or a hazardous scenario for the system. For a dynamic reliability assessment Prime Implicants (PIs) have to be identified, that ideally correspond to the MCSs of a static ET, but are also supplied

with the information of time, sequence and magnitude of failures occurrences[17]; moreover, also Near Misses (NMs) need to be identified (i.e., sequences among safe scenarios, whose sequences of events lead the safety parameter values close to, but not exceeding, the corresponding acceptable thresholds[3,21,22]).

The dynamic reliability analysis that will follow will show that one branch (scenario) of a static ET can actually evolve into a safe, a NM or a PI scenario, at the same time, of a RDET. In other words, we will show that a single branch (scenario) of a static ET corresponds effectively to more different branches in the RDET, which are all the possible combinations of timing, order and magnitude of the same failed components; consequently the reliability assessment done with a static ET might be misleading.

III. THE CASE STUDY

III.A. The U-Tube Steam Generator (UTSG) Model

A sketch of a U–Tube Steam Generator (UTSG) of a NPP is shown in Fig. 2. This system has been chosen because several studies have shown that its malfunction can be considered as one of the major causes of NPP unavailability[23–25].

The reactor coolant enters the UTSG at the bottom, moves upward and then downward in the inverted U-tubes, transferring heat to the secondary fluid before exiting at the bottom. The secondary fluid, the feed water (Q_e), enters the UTSG at the top of the downcomer, through the space between the tube bundle wrapper and the SG shell. The value of Q_e is regulated by a system of valves: a low flow rate valve, used when the operating power (P_o) is smaller than 15% of nominal power (P_n), and a high flow rate valve when $P_o > 0.15\ P_n$ [26]. In the secondary side of the tube bundle, water heats up, reaches saturation, starts boiling and turns into a two-phase mixture. The two-phase fluid moves up through the separator/riser section, where steam is separated from liquid water, and through the dryers, which ensure that the exiting steam (Q_v) is essentially dry[16]. The separated water is recirculated back to the downcomer. The balance between the exiting Q_v and the incoming Q_e governs the change in the water level in the SG. Because of the two-phase nature, two types of water level measurements are considered, as shown in Fig. 2, each reflecting a different level concept: the Narrow Range Level (N_{rl}) is calculated by pressure difference between two points close to the water level and indicates the mixture level, whereas, the Wide Range Level (W_{rl}) is calculated by pressure difference between the two extremities of the SG (steam dome and bottom of the downcomer) and indicates the collapsed liquid level that is related with the mass of water in the SG[16].

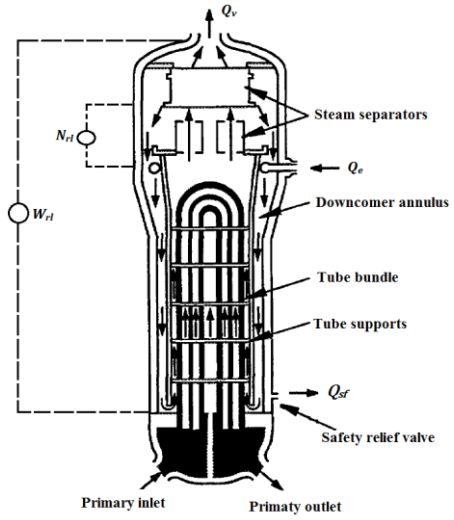

Fig. 2. Sketch of a UTSG of a NPP.

The goal of the system is to maintain the SG water level at a reference position (N_{ref}): the SG fails if the N_{rl} rises (falls) above (below) the threshold N_{high} (N_{low}), that trigger an automatic turbine trip. Indeed, if the N_{rl} exceeds N_{high}, the steam separator and dryer lose their functionality and excessive moisture is carried in Q_v, degrading the turbine blades profile and the turbine efficiency; if N_{rl} decreases below N_{low}, insufficient cooling capability of the primary fluid occurs. Similarly, the W_{rl}, is relevant for the cooling capability of the primary circuit[23]. Pre-alarms are triggered when N_{rl} exceeds N_{hl} (N_{ll}) if a small deviation from N_{ref} occurs or when N_{rl} exceeds N_{vh} (N_{vl}), when the deviation is large. Set points of N_{ref} and of N_{rl} depend on P_o, and, thus, also the alarms thresholds depend on P_o[16].

A dedicated model has been implemented in SIMULINK to simulate the dynamic response of the UTSG at different P_o values[16]. Both feedforward and feedback digital control schemes have been adopted. The feedback controller is a PID that provides a flow rate Q_{pid} resulting from the residuals between N_{rl} and N_{ref}, whereas the feedforward controller operates a safety relief valve that is opened if and only if N_{rl} exceeds the N_{hl}, and removes a constant flow safety flow rate (Q_{sf}).

III.B. The set of possible failures and repairs

The set of multiple component failures considered that can occur at random times during the system life (T_{miss} = 4000 s) are:

1. The outlet steam valve (ST.V) can fail in three different positions: i) closed; ii) stuck open at 50% of the nominal Q_v that should be provided at P_o, iii) stuck open at 150% of the nominal Q_v that should be provided at P_o.
2. The communication (COMM) between the sensor that monitors $\boldsymbol{N_{rl}}$ and the PID controller can fail returning the same input value of the previous time step.
3. The safety relief valve (SV) can fail at a uniform random value Q_{sf} in the range [0.5, 50.5] (kg/s).
4. The PID controller can fail providing a uniform random flow rate Q_{sf} belonging to [-18, 18] % of the nominal Q_e that should be provided at P_o.

Three components out of four have been assumed to be repairable (steam valve has been considered to be affected only by catastrophic and abrupt failure has been considered). For the repairable components, the grace period has, thus, been calculated by simulating the free evolution of system dynamics and by running the developed SIMULINK model with a single failure criterion: one component fails and the respective time for N_{rl} to reach N_{vh} (and the alarm to be triggered) is set equal to the grace time. We have calculated:

- $t_{g,SV}$ = 72 s;
- $t_{g,PID}$ = 40 s;
- $t_{g,COMM}$ = 25 s;

The repairs have been, then, implemented in the SIMULINK model. For each *i*-th component ($t_{g,i}$) we have sampled the repair time ($t_{r,i}$), from a uniform distribution between zero and the grace period, and we have compared it with the corresponding grace period ($t_{g,i}$) for the component. When $t_{r,i} < t_{g,i}$ the component has been considered as good as new, otherwise the component has been considered failed for the rest of the evolution of the scenario.
Choices and hypotheses for modeling the failures (i.e., the mission time, the number and type of faults, the distributions of failure times and magnitudes) have been arbitrarily made with the aim of generating multiple failures in the sequences and capturing the dynamic influence of their order, timing and magnitude on the accidental scenarios evolution[16]. In particular, the mission time (T_{miss} = 4000 s) has been chosen in order to account for the complete development also of slow dynamic accident scenarios[16].

III.C. The ET analysis

In this classical static reliability analysis, component failures are conservatively assumed to occur at the beginning of the scenario, with magnitudes equal to their extreme (either maximum or minimum) plausible values[21], with the scope of identifying the Minimal Cuts Sets (MCS) with respect to the high level failure modes. To identify the system MCS, the different system configurations have been simulated by the SIMULINK model at high and low (constant) power levels. Without loss of generality, the framework of analysis here presented focuses only on the high level failure mode of the system, neglecting the low level failure mode. It turns out that the MCSs for the high level failure mode are the same at both power levels (Fig. 3): the failure of the PID controller at its minimum values (i.e., -18% of the nominal Q_e that should be provided at P_o) and of the steam valve at its maximum value (i.e., 150% of the nominal Q_v value that should be provided at P_o) are two first order MCS[16].

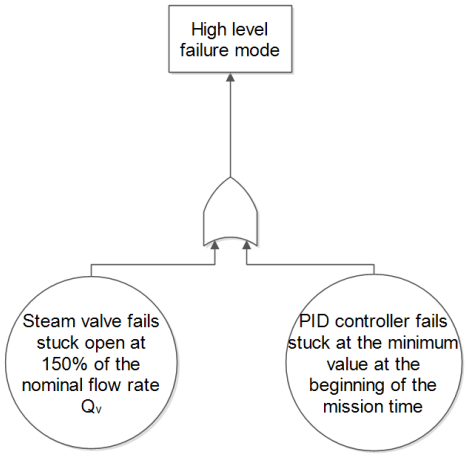

Fig. 3. Fault Tree for the high level failure mode.

Let us now assume a probability of 10^{-3} for the PID failure and the communication between the sensor and the PID failure ($P_{fail,PID}$ and $P_{fail,COMM}$), 10^{-2} for the steam valve failure ($P_{fail,ST.V}$) and 10^{-4} for the safety valve failure ($P_{fail,SV}$). Fig. 4 shows an ET for the scenario: Safety valve, Communication, PID and steam valve fail (or not) with this fixed order of failure occurrence, at the beginning of the mission time with the worst possible magnitude. The probability of each branch is given in Fig. 4: in particular, the probability of MCSs (whose branches are plotted in dotted lines) turns out to be equal to 1.097E-02.

Initiating Event	Safety valve		Communication		Steam valve		PID		Branch Probabiility
	No failure	9,999E-01	No failure	9,990E-01	No failure	9,900E-01	No failure	9,990E-01	9,879E-01
							Failure @time = 0 with max magnitude	1,000E-03	9,889E-04
					Failure @time = 0 with maximum magnitude	1,000E-02	No failure	9,990E-01	9,979E-03
							Failure @time = 0 with max magnitude	1,000E-03	9,989E-06
			Failure @time = 0 with maximum magnitude	1,000E-03	No failure	9,900E-01	No failure	9,990E-01	9,889E-04
							Failure @time = 0 with max magnitude	1,000E-03	9,899E-07
					Failure @time = 0 with maximum magnitude	1,000E-02	No failure	9,990E-01	9,989E-06
							Failure @time = 0 with max magnitude	1,000E-03	9,999E-09
	Failure @time = 0 with maximum magnitude	1,000E-04	No failure	9,990E-01	No failure	9,900E-01	No failure	9,990E-01	9,880E-05
							Failure @time = 0 with max magnitude	1,000E-03	9,890E-08
					Failure @time = 0 with maximum magnitude	1,000E-02	No failure	9,990E-01	9,980E-07
							Failure @time = 0 with max magnitude	1,000E-03	9,990E-10
			Failure @time = 0 with maximum magnitude	1,000E-03	No failure	9,900E-01	No failure	9,990E-01	9,890E-08
							Failure @time = 0 with max magnitude	1,000E-03	9,900E-11
					Failure @time = 0 with maximum magnitude	1,000E-02	No failure	9,990E-01	9,990E-10
							Failure @time = 0 with max magnitude	1,000E-03	1,000E-12

Fig. 4. Event Tree.

To build a RET, the repair times are assumed to be exponentially distributed with a repair rate μ equal to the inverse of the grace period. Therefore, under these assumptions, the repair probability, which is the probability that the repair time is less than the grace period is (for the i-th component):

$$P(t_{r,i} < t_{g,i}) = 1 - e^{-(\mu t)} = 0.63 \qquad (1)$$

The obtained RET is shown in Fig. 5, where its capability of considering not only the possibility of failure of the different components but also their repair is accounted in the branch probability quantifications.

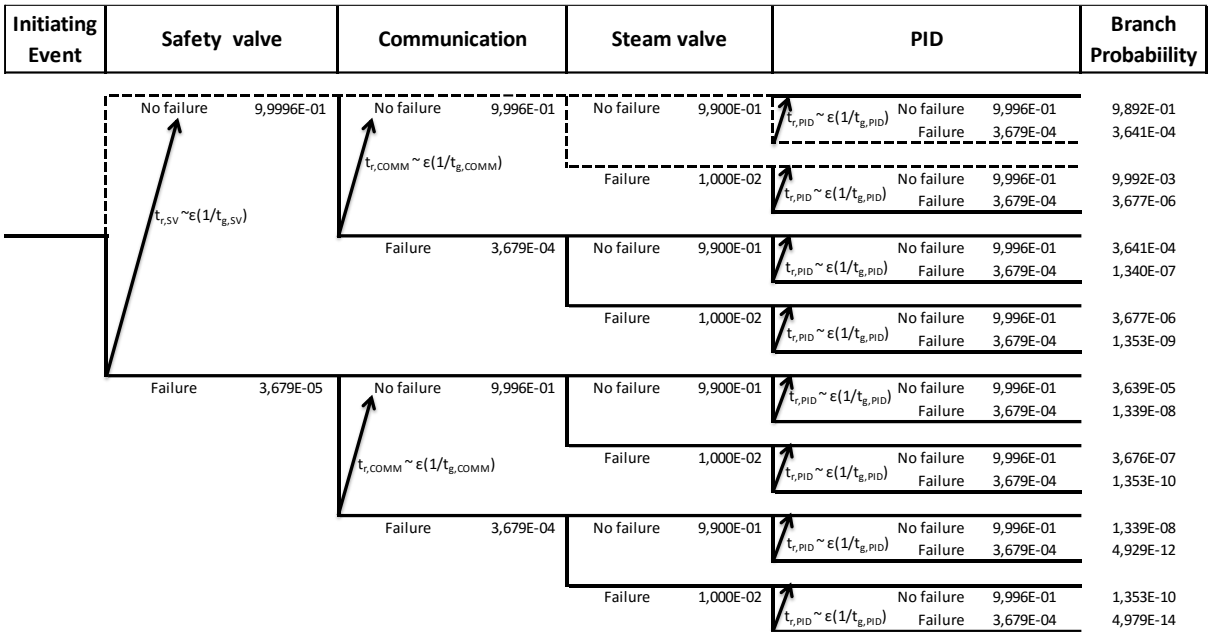

Fig. 5. Repairable Event Tree.

We notice that, the capability of modeling components repairs increases the probabilities of success branches and reduces the probabilities of failure branches, as expected. This shows that, when repairs are possible, the ET overestimates the probability of occurrence of failure branches, whereas RET results in a more realistic failure probability estimation. The sum of the branches probabilities corresponding to the MCS is, for the RET, 1.036E-02, which is much lower than the corresponding estimation provided by the ET.

III.D. Dynamic reliability analysis

Timing, order and magnitude of failures in reality can assume multi valued states and not only fixed values as in Section 3.3. This would make the problem intractable within a classical ET framework but not within a DET where we approximate the problem with discretized timing and magnitude of failure events in order to generate the dynamic scenarios. In particular, a Multiple Value Logic (MVL) for an approximated description of the continuous time of occurrence of component failures and their magnitudes has been adopted[16]. The MVL allows describing a situation in which the components can fail at any (discrete) time (not only the initial time) along the scenario, with different (discrete) magnitudes (not only the most conservative)[16]. The discretization of the time and magnitudes values is as follows:

- Time discretization: we refer to t=1, t=2, t=3 and t=4, for failures occurring in the intervals [0, 1000] (s), [1001, 2000] (s), [2001, 3000] (s), [3001, 4000] (s), respectively; if the label t=0, the component does not fail within the time of the whole scenario, T_{miss}
- Magnitude discretization:
  - the steam valve magnitude is indicated as 1, 2 or 3 for failure states corresponding to stuck at 0%, stuck at 50% and stuck at 150% of the Q_e value that should be provided at P_o, respectively; if the steam valve magnitude is indicated as 0, the component does not fail in T_{miss};
  - the safety relief valve fails with magnitude indicated as 1, 2, 3 and 4, if it is stuck between [0.5, 12.6] (kg/s), (12.6, 25.27] (kg/s), (25.27, 37.91] (kg/s) and (37.91, 50.5] (kg/s), respectively; if the safety relief valve magnitude is indicated as 0, the component does not fail in T_{miss},
  - the communication between the sensor measuring N_{rl} and the PID controller is labeled 0 if the communication works, 1 otherwise;

– the PID controller failure magnitude range is discretized into 8 equally spaced magnitude intervals, labeled from 1 to 8, representative of failure states corresponding to discrete intervals of output value belonging to [-18,18]% of the Q_e value that should be provided at P_o, if the PID controller magnitude is labeled as 0, the component does not fail in T_{miss}.

All possible MVL sequences are, therefore, 100509. In fact, the arising dynamics leads the 16 failure branches of the ET of Fig. 4 to reach 360 by spooning each branch according to the different failure magnitudes of the components whose failure occurs along the scenario: when the safety valve fails, for example, failure branches will be four (being four its possible failure magnitudes); similarly, when the steam valve fails failure branches will be three; there will be eight possible failure branches for the PID, whereas a single failure magnitude is considered when the communication fails. When also timing is considered in the dynamics, the branches of the ET turn out to be 100509.

To show the capability of a RDET to account for dynamic aspects in the evolution of the accidental scenarios, without loss of generality, we focus our analysis on a selection of MVL sequences that, incidentally, are three safe sequences, four NMs and four PIs, among the 100509 possible sequences (the interested reader can refer to[16] where the characterization of sequences in safe, NMs and PIs is presented). TABLE 1 shows the selected sequences (defined in terms of order, magnitude and timing of failure for each component).

TABLE I: The MVL dynamic sequences considered for the comparison of ET and RDET.

	Safety valve			Communication			PID			Steam valve		
Sequence	Time	Mag	Order	Time	Mag	Order	Time	Mag	Order	Time	Mag	Order
SAFE	0	0	0	4	1	2	4	8	1	0	0	0
SAFE	1	3	2	1	1	1	4	3	3	0	0	0
SAFE	4	3	4	2	1	3	2	5	1	2	2	2
NM	3	3	2	4	1	3	2	4	1	0	0	0
NM	4	4	3	4	1	2	1	4	1	0	0	0
NM	4	3	4	4	1	3	1	4	1	2	1	2
NM	4	2	3	2	1	2	1	4	1	0	0	0
PI	1	1	1	0	0	0	3	4	2	0	0	0
PI	1	4	1	3	1	3	1	2	2	0	0	0
PI	2	3	1	4	1	2	4	3	3	0	0	0
PI	2	4	1	3	1	4	3	4	3	2	3	2

Fig. 6 reports, for each dynamic sequence, the values of the probability of the corresponding branch in the static ET of Fig. 4 and that of the RET of Fig. 5. Additionally, Fig. 6 shows the probability calculated with a RDET that accounts for the different magnitudes by considering the PID failure probability $P_{fail,PID}$ equal to 1.25E-04 (i.e, 1/8 of the $P_{fail,PID}$ in the static ET), the safety valve failure probability $P_{fail,SV}$ equal to 2.5E-05 (i.e, 1/4 of the $P_{fail,SV}$ in the static ET), the steam valve failure probability $P_{fail,ST.V}$ equal to 3.33E-03 (i.e., 1/3 of the $P_{fail,ST.V}$), and $P_{fail,COMM}$ has been assumed still to be equal to 10^{-2}. Fig. 6 also shows the failure probability of the system when any of the considered sequences occurs under the hypotheses of not repairable and in repairable cases, P_F and $P_{F,rep}$ respectively.

This has been done by sampling magnitudes and time of failures from the corresponding interval (e.g. if the time of failure t is equal to 1, corresponding failure time has been sampled in the interval [1, 1000]), and the SIMULINK model has been run 100 times for each sequence.

We can notice that dynamic effects of timing and order of failures are evident if we consider, for example, the sequence "safety valve failure magnitude equal to 3, failure magnitude of the communication equal to 1, steam valve not failed (failure magnitude equal to 0) and failure magnitude of the PID controller equal to 3" (corresponding to the second and the tenth sequence of

I): the originated DET branches are differing only for timing and order of failure events but lead either safe or PI even though the failure magnitudes are the same.

Moreover, we can claim that for each dynamic sequence, static methods seem to overestimate the branch failure probability because each branch of a static ET condenses all the combinations of order, timing and magnitude, for the same failed

components. Our aim is, therefore, to verify whether, considering all the dynamic sequences spooned by the same static branch, ET overestimates the failure probability. To do this, we consider the PI sequence Table II.

This sequence corresponds, in the static ET of Fig. 4, to the branch where safety valve and PID fail, whereas the communication between the sensor and the PID controller and steam valve do not fail, resulting in a branch probability of occurrence equal to 9.89E-08. In the RET of Fig. 5, it corresponds to the branch where safety valve and PID fail (and can be repaired), whereas the communication between the sensor and the PID controller and steam valve do not fail, resulting in a branch probability of occurrence equal to 1.33E-08.

TABLE III lists all the dynamic sequences that are lumped in one branch of the ET and RET that should, instead, considered for calculating the branch probability of the RDET.

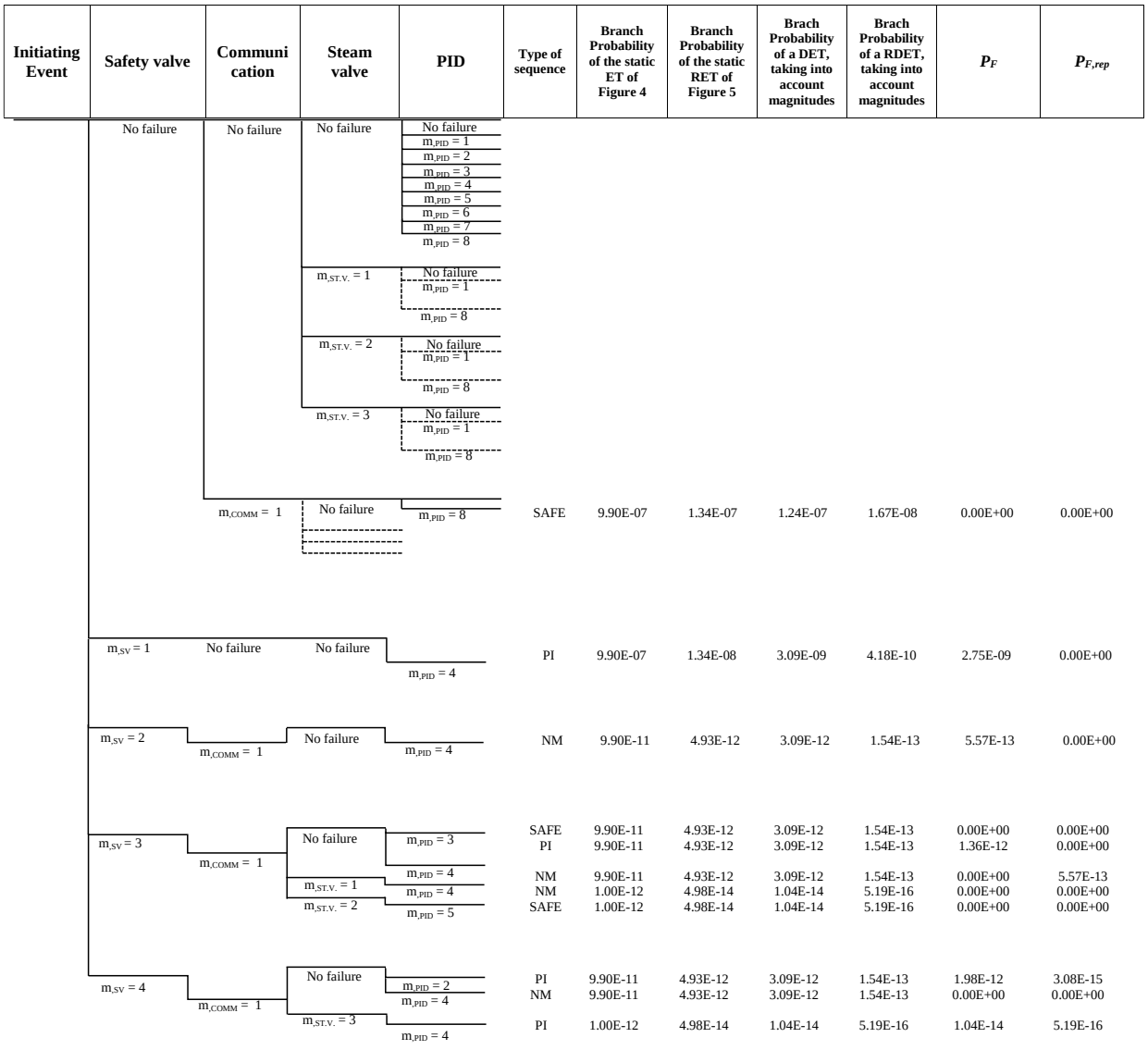

Fig. 6. Comparison of the results for the dynamic sequences of I.

TABLE II: MVL of the selected sequence.

Safety valve			Communication			PID			Steam valve		
Time	Mag	Order	Time	Mag	Order	Time	Mag	Order	Time	Mag	Order
1	1	1	0	0	0	3	4	2	0	0	0

For each dynamic sequence (i.e., each row of TABLE III), the probability of system failure P_F has been calculated based on a set of 100 runs of the SIMULINK model with random times of failures sampled from the corresponding interval and $P_{fail,PID,}$ the PID failure probability, equal to 1.25E-04 (i.e, 1/8 of the $P_{fail,PID}$ in the static ET), whereas $P_{fail,SV,}$ the safety valve failure probability, equal to 2.5E-05 (i.e, 1/4 of the $P_{fail,SV}$ in the static ET).

TABLE III: Simulation results for all the possible combinations.

		Not Repairable case			Repairable case		
Mag Safety	Mag PID	Branch probabilities in the static ET of Fig. 4	P_F	P_F | *sequence*	Branch probabilities in the static ET of Fig. 5	$P_{F,rep}$	$P_{F,rep}$|*sequence*
1	1	9.89E-08	1	3.09E-09	1.34E-08	0.13	5.44E-11
1	2	9.89E-08	1	3.09E-09	1.34E-08	0.01	4.18E-12
1	3	9.89E-08	1	3.09E-09	1.34E-08	0	0.00E+00
1	4	9.89E-08	0.89	2.75E-09	1.34E-08	0	0.00E+00
1	5	9.89E-08	0	0	1.34E-08	0	0.00E+00
1	6	9.89E-08	0	0	1.34E-08	0	0.00E+00
1	7	9.89E-08	0	0	1.34E-08	0	0.00E+00
1	8	9.89E-08	0	0	1.34E-08	0	0.00E+00
2	1	9.89E-08	1	3.09E-09	1.34E-08	0.17	7.11E-11
2	2	9.89E-08	1	3.09E-09	1.34E-08	0	0.00E+00
2	3	9.89E-08	0.96	2.97E-09	1.34E-08	0	0.00E+00
2	4	9.89E-08	0.17	5.25E-10	1.34E-08	0	0.00E+00
2	5	9.89E-08	0	0	1.34E-08	0	0.00E+00
2	6	9.89E-08	0	0	1.34E-08	0	0.00E+00
2	7	9.89E-08	0	0	1.34E-08	0	0.00E+00
2	8	9.89E-08	0	0	1.34E-08	0	0.00E+00
3	1	9.89E-08	1	3.09E-09	1.34E-08	0.2	8.37E-11
3	2	9.89E-08	1	3.09E-09	1.34E-08	0	0.00E+00
3	3	9.89E-08	0.29	8.96E-10	1.34E-08	0	0.00E+00
3	4	9.89E-08	0	0	1.34E-08	0	0.00E+00
3	5	9.89E-08	0	0	1.34E-08	0	0.00E+00
3	6	9.89E-08	0	0	1.34E-08	0	0.00E+00
3	7	9.89E-08	0	0	1.34E-08	0	0.00E+00
3	8	9.89E-08	0	0	1.34E-08	0	0.00E+00

4	1	9.89E-08	1	3.09E-09	1.34E-08	0.2	8.37E-11
4	2	9.89E-08	0.48	1.48E-09	1.34E-08	0.02	8.37E-12
4	3	9.89E-08	0	0	1.34E-08	0	0.00E+00
4	4	9.89E-08	0	0	1.34E-08	0	0.00E+00
4	5	9.89E-08	0	0	1.34E-08	0	0.00E+00
4	6	9.89E-08	0	0	1.34E-08	0	0.00E+00
4	7	9.89E-08	0	0	1.34E-08	0	0.00E+00
4	8	9.89E-08	0	0	1.34E-08	0	0.00E+00

Results show that the probabilities that the system fails given that PID and steam valve fail sum up to 3.33E-08 and 3.05E-10 (for the non repairable and repairable case, respectively) that are smaller than the probability of the lumped branches of the ET and RET.

However, it may happen that (if the system is non–coherent), when considering all the dynamic sequences (instead of being lumped), the estimate of the failure probability may be larger than that obtained with an ET or a RET, because of the neglection of the non–coherency phenomena of system failure when components are repaired.

IV. CONCLUSIONS

In this paper, we have compared the results of an ET, a RET and a RDET when applied for the reliability assessment of a UTSG of a NPP. We have shown the advantages of a RDET among the others, because of the capability of integration of DET and RET methodologies. The analysis stresses the importance of accounting for dynamic effects into the scenarios modelling: the same type of events but occurring at different times can lead the system to different end states. Finally, we can claim that if we consider a static sequence to be, then, spooned in many sequences in a RDET, the static ET overestimates the probability of failure of the system.

REFERENCES

1. International Atomic Energy Agency (IAEA). *Deterministic Safety Analysis for Nuclear Power Plants: Safety Guide*.; 2008.
2. Aldemir T. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. *Ann Nucl Energy*. 2013;52:113-124. doi:10.1016/j.anucene.2012.08.001.
3. Zio E. Integrated deterministic and probabilistic safety assessment: Concepts, challenges, research directions. *Nucl Eng Des*. 2014;280:413-419. doi:10.1016/j.nucengdes.2014.09.004.
4. Marchand S., Tombuyses B. LP. DDET and Monte Carlo simulation to solve some dynamic reliability problems. In: *Proceedings of the Fourth International Conference on Probabilistic Safety Assessment and Management (PSAM IV)*. New York; 1998:2055-2060.
5. Hofer E, Kloos M, Krzykacz-Hausmann B, Peschke J, Woltereck M. An approximate epistemic uncertainty analysis approach in the presence of epistemic and aleatory uncertainties. *Reliab Eng Syst Saf*. 2002;77(3):229-238. doi:10.1016/S0951-8320(02)00056-X.
6. Hofer E., Kloos M., Krzykacz-Hausmann B., Peschke J. SM. Dynamic Event Trees for Probabilistic Safety Analysis. In: *GRS, Garsching*. Germany; 2004.
7. Amendola A, Reina G. DYLAM-1: a software package for event sequence and consequence spectrum methodology. 1984. http://inis.iaea.org/Search/search.aspx?orig_q=RN:16081922. Accessed July 27, 2016.
8. Cacciabue PC, Amendola A, Cojazzi G. DYnamic Logical Analytical Methodology versus Fault Tree: the case study of the Auxiliary FeedWater system of a Nuclear Power Plant. *Nucl Technol*. 1986;74(2):195-208.
9. Cojazzi G. The DYLAM approach for the dynamic reliability analysis of systems. *Reliab Eng Syst Saf*. 1996;52:279-296. doi:10.1016/0951-8320(95)00139-5.
10. Acosta C, Siu N. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. *Reliab Eng Syst Saf*. 1993;41(2):135-154. doi:10.1016/0951-8320(93)90027-V.
11. Deoss, D., Siu N. A Simulation Model for Dynamic System Availability Analysis. 1989.
12. Izquierdo JM, Hortal J, Sánchez M, Meléndez E. Automatic Generation of Dynamic Event Trees: A Tool for Integrated Safety Assessment (ISA). In: Aldemir T, Siu NO, Mosleh A, Cacciabue PC, Göktepe BG, eds. *Reliability and Safety*

Assessment of Dynamic Process Systems. Berlin, Heidelberg: Springer Berlin Heidelberg; 1994:135-150. doi:10.1007/978-3-662-03041-7_10.

13. Vorobyev Y, Kudinov P. Development and application of a genetic algorithm based dynamic pra methodology to plant vulnerability search. In: *International Topical Meeting on Probabilistic Safety Assessment and Analysis 2011, PSA 2011*. Vol 1. ; 2011:559-573. http://www.scopus.com/inward/record.url?eid=2-s2.0-80051997967&partnerID=tZOtx3y1.
14. F. Di Maio, S. Baronchelli, E. Zio, "Hierarchical differential evolution for minimal cut sets identification: Application to nuclear safety systems", *Eur J Oper Res*., 238(2):645-652 (2014), doi:10.1016/j.ejor.2014.04.021.
15. 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 Trans Reliab*., 60(2):415-425, (2011), doi:10.1109/TR.2011.2134230.
16. F. Di Maio, M. Vagnoli, E. Zio, "Risk-Based Clustering for Near Misses Identification in Integrated Deterministic and Probabilistic Safety Analysis", *Sci Technol Nucl Install*., 1-29 (2015), doi:10.1155/2015/693891.
17. F. Di Maio, S. Baronchelli, E. Zio, "A Computational Framework for Prime Implicants Identification in Noncoherent Dynamic Systems", *Risk Anal*., 35(1):142-156, (2015), doi:10.1111/risa.12251.
18. Garribba S, Guagnini E, Mussio P. Multiple-Valued Logic Trees: Meaning and Prime Implicants. *IEEE Trans Reliab*. 1985;R-34(5):463-472. doi:10.1109/TR.1985.5222234.
19. Kumar R, Bechta S, Kudinov P, Curnier F, Marquès M, Bertrand F. A PSA Level-1 method with repairable components: An application to ASTRID Decay Heat Removal systems. In: *Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014*. ; 2015:1611-1617. http://www.scopus.com/inward/record.url?eid=2-s2.0-84906679503&partnerID=tZOtx3y1.
20. Karanki D.R., Dang V.N. MMT. Uncertainty propagation in Dynamic Event Trees - Initial results for a modified tank problem. In: *PSAM 2014 - Probabilistic Safety Assessment and Management*. ; 2014.
21. E. Zio, F. Di Maio, "Processing dynamic scenarios from a reliability analysis of a nuclear power plant digital instrumentation and control system", *Ann Nucl Energy*,36(9):1386-1399 (2009). doi:10.1016/j.anucene.2009.06.012.
22. F. Di Maio, M. Vagnoli, E. Zio, "Transient identification by clustering based on Integrated Deterministic and Probabilistic Safety Analysis outcomes", *Ann Nucl Energy*, 87:217-227 (2016). doi:10.1016/j.anucene.2015.09.007.
23. Kothare MV, Mettler B, Morari M, Bendotti P, Falinower C-M. Level control in the steam generator of a nuclear power plant. *IEEE Trans Control Syst Technol*. 2000;8(1):55-69. doi:10.1109/87.817692.
24. Habibiyan H, Setayeshi S, Arab-Alibeik H. A fuzzy-gain-scheduled neural controller for nuclear steam generators. *Ann Nucl Energy*. 2004;31(15):1765-1781. doi:10.1016/j.anucene.2004.03.014.
25. Marseguerra M, Zio E, Cadini F. Optimized adaptive fuzzy controller of the water level of a pressurized water reactor steam generator. *Nucl Sci Eng*. 2007;155(3):386-394.
26. Aubry J.,F., Babykina G, Barros A, et al. *Project APPRODYN: APPROches de La Fiabilité DYNamique Pour Modéliser Des Systèmes Critiques*.; 2012.