AN INTEGRATED MODELLING FRAMEWORK FOR COMPLEX SYSTEMS SAFETY ANALYSIS

Silvia Tolo*[1] and John Andrews[1]

[1]Resilience Engineering Research Group, University of Nottingham, UK

* Corresponding author: silvia.tolo@nottingham.ac.uk

This work was funded by the Lloyd's Register Foundation, with the project *Next Generation Prediction Methodologies and Tools for System Safety Analysis.*

Abstract

The ever-increasing complexity of engineering systems has fuelled the need for novel and efficient computational tools able to enhance the accuracy of current modelling strategies for industrial systems. Indeed, traditional Fault and Event Tree techniques still monopolize the reliability analysis of complex systems despite their limitations, such as the inability to capture underlying dependencies between components or to include degradation processes and complex maintenance strategies into the analysis. However, the lack of alternative solutions able to tackle large scale modelling efficiently has contributed to the continued use of such methodologies, together with their robustness and familiarity well rooted in engineering practice. The current paper defines a novel modelling framework for safety system performance which retains the capabilities of both Fault and Event Tree methods, but also overcomes their limitations. The ambition is to provide a technique for application to real-world systems preserving a familiar user-model interface and grounding the novel approach in well-known and established reliability techniques. In order to describe the methodology developed and demonstrate its validity, five case-studies referring to a simplified industrial plant cooling system are analysed and discussed. Further discussion regarding the scalability of the proposed approach is provided, outlining the advantages of the current implementation and its computational cost.

1 Introduction

Risk modelling methodologies have played a crucial role in the development and safe operation of engineering systems, allowing to understand their behaviour and to manage their growing complexity. Nevertheless, conventional approaches such as Fault and Event Trees (FT/ET), were developed back in the 1970s and have limitations in terms of their applicability to modern systems. Such limitations are intrinsically linked to the simplifying assumptions of the constancy of components failure rates and their independence. Both these hypothesis affect the ability of the model to capture the realistic system behaviour. In the case of constant failure rates, this results in the adoption of the exponential distribution for the representation of component failure time and may lead to the misrepresentation of the actual deterioration process to which systems are unavoidably subject. This may result in the overestimation of failure probability (e.g. in the case of decreasing failure rates) and hence overengineering, or in the underestimation of risks (e.g. in the case of increasing failure rates and aging components). Similarly, disregarding the dependencies influencing the performance of multiple components or subsystems, may conceal failure mechanisms or their significance for the overall system's safety, preventing an adequate understanding of the system's behaviour.

Several research efforts have been focused on overcoming the limitations of fault and event trees [22], leading to the development of dynamic FTs [10] [8], Boolean logic Driven Markov Processes [5] and Pandora temporal FTs [31], relying on the use of dynamic gates for modelling sequence dependent failure mechanisms and their computation through the use of Markov Models (MM) [12]. However, such solutions come with a wide range of shortcomings and remain mostly restricted to academic applications or to small-scale problems, due to the computational burden generally associated with this kind of techniques [17] [30] [32]. The objective of the research presented in this paper is to address the need for novel approaches to safety analysis able to expand the capacity of existing techniques and complement traditional risk assessment methodologies. While FT/ET come with limitations, it is also true that they have played a crucial role in the successful design and operation of complex engineering systems for decades, and remain the common language shared between designers, analysts and regulators. The aim is then to implement a modelling framework able to enhance the strengths of traditional techniques (e.g. modelling simplicity, relatively low

computational costs, robustness), by overcoming the limitations. In the proposed methodology, this is achieved by identifying the sections of the model where underlying traditional assumptions are unjustified and adopting numerical techniques better suited for their assessment. The approach implies the integration of several existing techniques, such as FTs, ETs, MMs [16], Binary Decision Diagrams (BDDs) [9] and Petri Nets (PNs) [20], under the same framework. The novel technique can be applied to any system requiring FT/ET analysis, providing the analyst with a higher degree of modelling flexibility.

More detail regarding the structure and nature of the proposed modelling framework is provided in Section 2. The validity and efficiency of the proposed framework is then tested through its application to a simplified industrial system, whose description is provided in Section 3. Five case-studies are then considered, in order to compare the proposed solution with traditional techniques for several types of system dependencies. Finally, Section 4 is dedicated to discussing the computational feasibility of the proposed approach for large scale systems.

2 Methodology

Large-scale engineered systems consist of many concurrently operating elements, which interacting as an ensemble provide the designed system functionality. The malfunctioning of one or more of such elements can hinder the correct operation of systems, which are therefore vulnerable to faults due to their spatial distribution and subsystems interdependencies [4]. The resulting emergent and multiscale properties of large engineered systems have often earned them the classification of complex systems [6], although there is no widely agreed upon definition of what makes an engineering system complex [23].

The use of the term complexity in this study is strictly intended from a reliability modelling point of view, and refers to those dynamic features of systems, e.g. degradation processes, stochastic dependencies, feed-forward and feedback connections, that are not representable through traditional tools. Indeed, the most straightforward approach to model the failure of engineering systems is to interpret these latter as a network of interconnected and intercommunicating components. Under this assumption, the losses of functionalities in the system can be mapped through the so called

Fault Trees [2]: such graphical tools allow to factorize the main system functionality in terms of sub-functionalities (e.g. through component operational state), defining the logical rules regulating the interaction between the nodes of the tree/network and hence the systems components. While this approach has been adopted successfully in the safety analysis of large-scale engineered systems [24], it relies on the strong simplifying assumption of components independence, hence neglecting the dynamic features that are proper of real-world systems. Still, the behaviour of complex stochastic systems is determined by dynamic logical interactions between components (e.g. synchronization, sequentiality, concurrency and conflict), as therefore must be their reliability.

The modelling framework proposed in this study aims at overcoming these limitations, allowing the accurate representation of actual complex dynamic features of the system within the FT formalism. This is achieved through the integration into the latter of techniques suitable for the depiction of components interaction in time [3] [13] [15]. The key to such integration is the use of common probabilistic formalism, able to translate the behaviour of the systems and its components on different modelling levels: the components level, which can be characterized by complex, dynamic interactions which are quantified probabilistically through the use of PNs and MMs; and the system functionality level, where the information collected previously is re-introduced in terms of its probabilistic contribution to the overall system loss of functionality over the time interval of study, with regards to which is a static value.

This results in a novel simulation framework that, rooted in well-established mathematical modelling formulations, extends the capabilities of current risk analysis methods, overcoming their most critical limitations. The hope is very much to promote through similar tools a significant shift towards more realistic system modelling, without renouncing the familiarity of techniques already deeply entrenched in engineering practice.

The proposed solution relies on integration of traditional FT/ET with PNs and MMs, marrying computational feasibility with analysis accuracy. An overview of the simulation framework implemented is presented in Figure 1. The input required from the analyst consists of the system setting (in the form of conventional FTs and ETs as well as component failure modes) and, where necessary, of PN/MM models representing complex components' maintenance strategies and dependencies. The developed algorithms identify and isolate independent modules within individual or combined (in

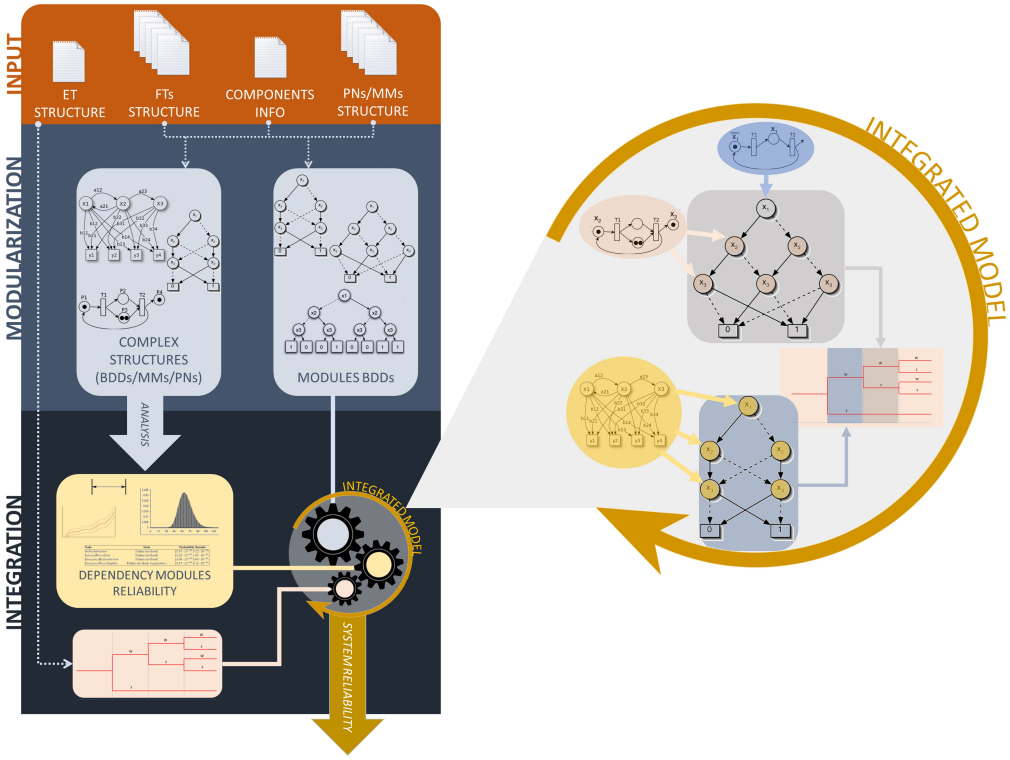


Figure 1: Overview of the proposed simulation framework

the case of dependencies between subsystems) fault trees containing Dependency Groups (DGs). These refer to closed sets of components whose failures are mutually dependent on each other. The isolated complex structures are then implemented (when not pre-defined by the user) and analysed in the form of individual PNs or MMs, generating a high level of detail in the simulation. Finally, the results obtained are re-integrated within the original FT structure and subsequently within the ET, completing the analysis. The following sections provide a detailed description of the computational steps entailed by the methodology.

2.1 Input Structure

The first step towards the generation of models for the proposed methodology is the submission of:

- system event tree structure: this provides crucial information on the nature of the interaction between subsystems, capturing how their failure or working states impact the safety of the overall system of interest.
- subsystems fault tree structures: these represent the causes of failure patterns resulting from the malfunctioning of the subsystem's components.
- components failure mode information: a complete list of the system's components and their associated failure/repair/inspection time distributions.
- PNs/MMs models: these provide user-defined PN or MM structures modelling complex features of the system (such as complex maintenance strategies or degradation processes), offering a further degree of flexibility to the overall methodology.

Figure 2 gives an overview of the input structure and its implementation in the analysis.

2.2 Components Reliability Metrics Computation

The first step of the procedure involves the calculation of the reliability metrics, i.e. failure frequency and unavailability, associated with each system component. Where conventional assumptions, such as constant failure and repair rates components, independence and simplistic maintenance strategies, are relevant, the unavailability and failure frequency of the component is calculated according to

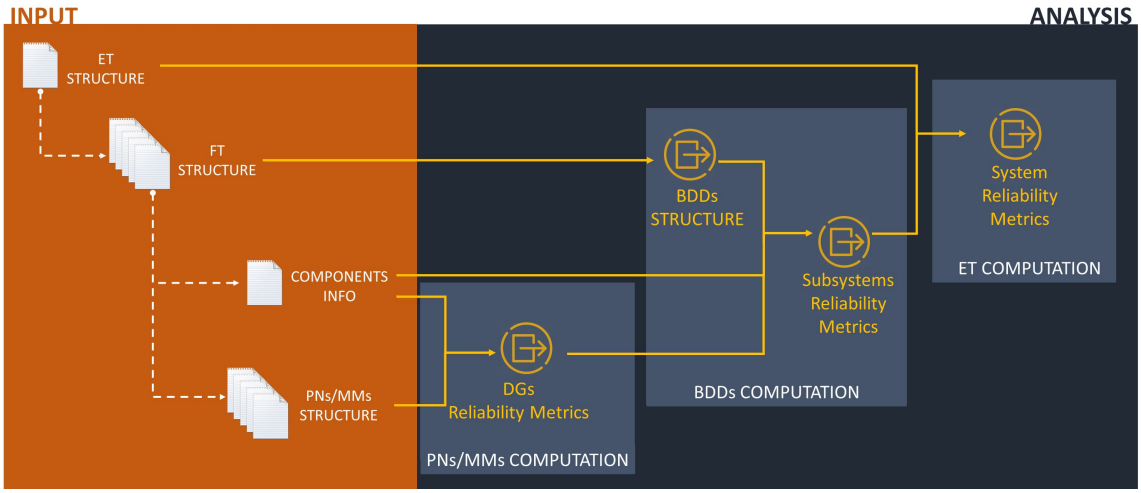


Figure 2: Hierarchical input structure and analysis organisation

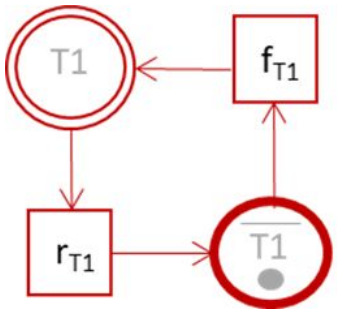


Figure 3: PN model of components $T1$ failure-repair cycles

traditional failure models [2]. Conversely, when failure and repair times are represented by distributions other than exponential, the proposed approach relies on the use of PNs. These are utilised to compute the component's unavailability and failure intensity simulating the stochastic occurrence of alternating failure and repair events. For instance, let the failure time of a component T1 be represented by a Weibull distribution, hence having a non-constant failure rate. In addition, assume the repair time associated with T1 to be lognormally distributed. The resulting PN model portraying the failure mode of $T1$ is shown in Fig. 3. The network consists of two places: one associated with the correct operation of the component (labelled $\overline{T1}$), the other ($T1$) indicating its failure state. The presence of a token in one or the other place denotes the current state of the component. The firing of the stochastic failure transition, occurring at time f_{T1}, causes the movement of the token from

the working to the failure state, while the repair transitions (occurring at time r_{T1}) simulates the completion of corrective maintenance and hence the restoration of component functionality.

In the framework implementation, similar life-cycle PNs are automatically generated for any component in input characterised by non-traditional failure models, and then simulated to convergence. The component unavailability information is then extracted from the simulation results, being calculated as the fraction of downtime over the total simulation time. The failure intensity is estimated as the number of failures occurring over the simulated time interval. More complex maintenance strategies or degradation processes affecting the component can be captured through the same approach: complex features may be captured by user-defined models provided in input, through the use of PN or MM structures. The use of MMs in particular can offer advantages in the case exponentially distributed failure and repair times, since the associated steady-state solution may reduce the computational demand associated with the calculation. Nevertheless, it is worth emphasizing that even the use of more expensive simulation techniques (i.e. PN) is restricted only to those components for which traditional simplifying assumptions are unjustified and thus resulting in potential inaccuracies, while computational ease is maintained untouched for the remaining components.

2.3 Dependency Groups Identification and Computation

The unavailability and failure intensity of dependent components, is estimated in relation to the DG to which they belong. This is achieved through the implementation and computation of PNs or MMs models representing the dependency relationship, resulting in the estimation of the joint failure probability and intensity associated with the components included in the group.

For instance, with reference to Fig.4, let $P1$ and $P2$ be two stochastically dependent components (pumps): these share the load equally but when one fails and the remaining functioning component must supply the required flows alone. Under these conditions the functioning pump experiences a higher load and is more likely to fail.

If both components are in working order (places $\overline{P1}$, $\overline{P2}$), their failure time is represented by the distributions f_{P1} and f_{P2} respectively. However, when $P1$ fails (place $P1$), the redundant component $P2$ experiences a greater load. This increases its failure probability, changing the failure time distribution from f_{P2} to f'_{P2} (see transitions named accordingly in Fig. 4). Symmetrically, if $P2$

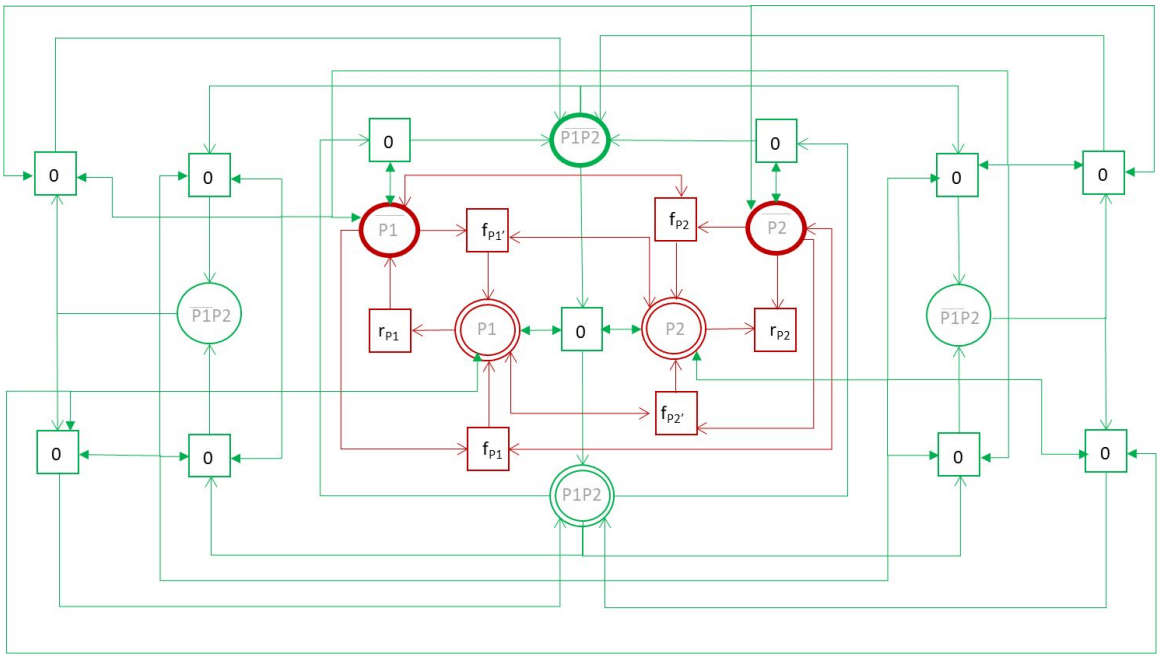


Figure 4: PN modelling the dependency group embracing components $P1$ and $P2$

fails (place $P2$), the failure time distribution for the component $P1$ increases from f_{P1} to f'_{P1}. The relationship between the two components $P1$ and $P2$, is then fully captured by the PN in Fig. 4. The simulation of the latter is carried out using the Monte Carlo method [21] and results in the computation of the joint reliability metrics of interest for the two components: for example, the joint availability can be calculated dividing the simultaneous working time of the two components (i.e. token in the joint place $\overline{P1P2}$) over the simulated time interval. Similarly, the failure intensity of the event $\overline{P1}P2$, referring to the working state of $P1$ and failure state of $P2$, can be calculated as the number of times a token entered the associated place $\overline{P1}P2$ over the total simulated system life. If all the residence times in any state of the model are exponentially distributed, the failure mechanisms within the dependency group could be represented through the use of a MM, quantifying the joint probabilities of interested through the computation of its steady-state solution. This alternative approach may reduce the computational effort when compared to the equivalent PN, hence enhancing the efficiency of the calculation. Figure 5 shows the MM associated with the DG entailing $P1$ and $P2$, where $\lambda 1$ and $\lambda 2$ refer to the rates associated with the failure of one component experienced when the second component is working or failed respectively, while ν indicates the repair

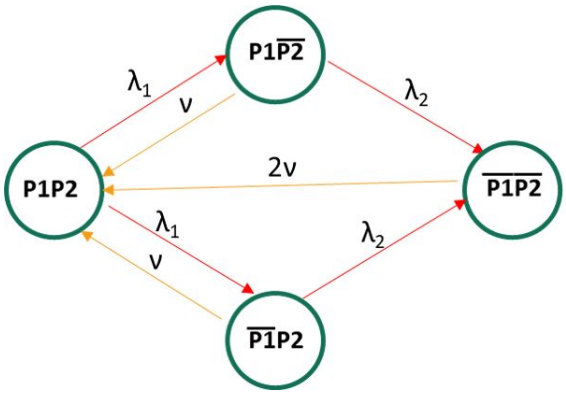


Figure 5: MM modelling the dependency group embracing components P1 and P2

rate common to the two components. This step of the methodology is comparable to the procedure discussed in Section 2.2 for non-conventional component failure models, with the only difference that the simulation, and subsequently its output, are here referring to a group of dependent components rather than to individual, independent ones.

2.4 FTs identification and Conversion

The next phase of the procedure focuses on the identification of independent system FTs and their conversion into equivalent BDDs. If all subsystems are independent, the FTs submitted in input remain untouched. Conversely, if any type of dependency exists between two or more subsystems, the respective FTs are merged together. This operation is carried out directing the top events of the individual dependent FTs into an AND gate whose output becomes the top event of the new merged FT.

For example, let $X1$ and $X2$ be the top events of two individual FTs representing the failure of a primary and secondary cooling subsystem respectively (see Fig. 7). Assuming the two subsystems to have a common component $P2$, the related FTs fail the assumption of independence, resulting in the need to compute the two models jointly and hence to merge the two FTs as shown in Fig. 6. Overall, the result of this step is to obtain a set of independent FT models, that can then be analysed separately without affecting the accuracy of the analysis.

Once the independent FTs are identified, their conversion to BDDs is carried out. A BDD is a

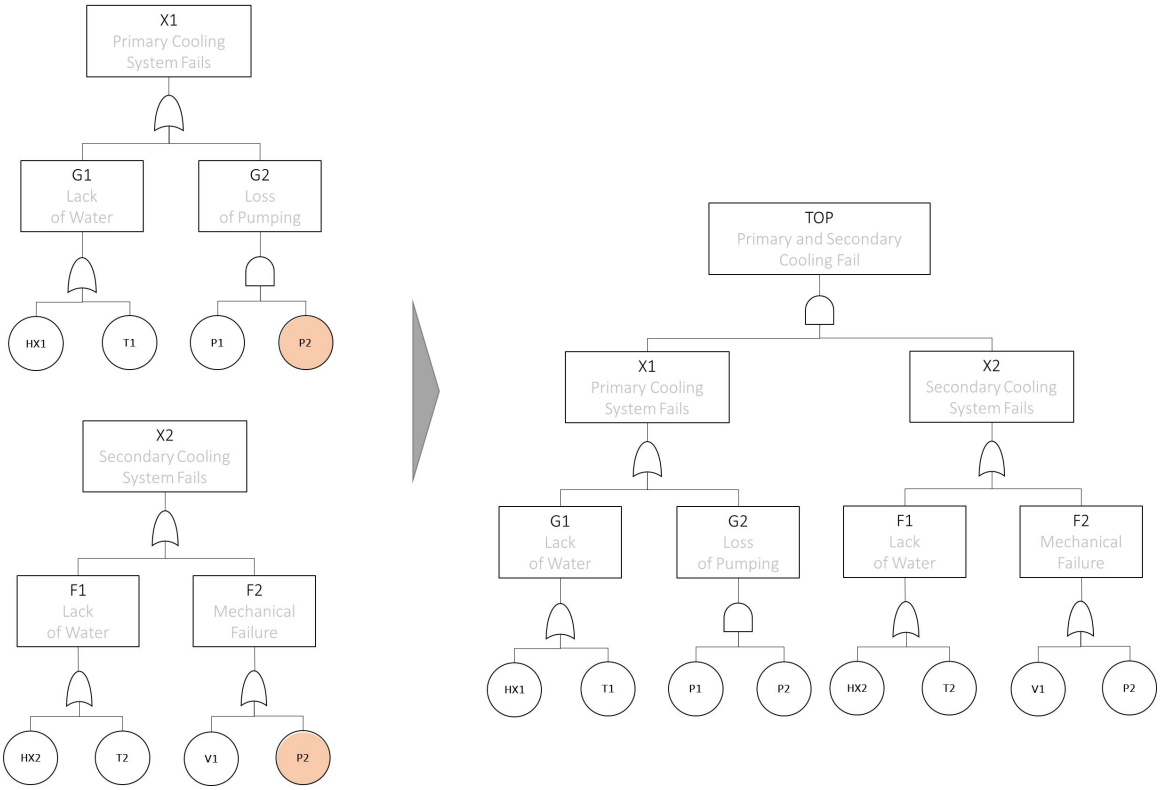


Figure 6: Merging procedure for dependent FTs

directed acyclic graph consisting of terminal and non-terminal vertices connected by edges (also referred to as branches) [19] [9]. Each non-terminal vertex is associated with a basic event (e.g. the failure of individual components in the current application) and is the origin of two branches: a 0 branch representing the non-occurrence of the basic event (e.g. the working state of the component) and a 1 branch representing the occurrence of the basic event (e.g. component failure). Terminal vertices, in which all paths through the BDD terminate, assume either a 0 value, associated with the working state of the system, or 1, indicating instead the failure of the system. The Boolean function underlying a BDD structure can be factorised node by node through the use of $if-then-else$ (ite) structure. Any BDD node N can be represented as:

$$N = ite(X_i, G1, G0) \tag{1}$$

where X_i, which labels the node, refers to the associated basic event, while $G1$ and $G0$ are further Boolean function representing children nodes lying on the 1 and 0 branch of N respectively. The expression in Eq. 1 translates as: *if* X_i fails *then* consider the Boolean function *G1*; else consider function *G0* which, lying on the branch 0, implies the working state of the same component [26]. The structure of the BDD can be then expressed as the combination of the *ite* structure of its nodes. For instance, the structure of the BDD shown on the right hand-side of Fig. 10a, can be expressed as:

$$N_{root} = ite\left(HX1, 1, ite\left(T1, 1, ite\left(P2, ite\left(P1, 1, 0\right), 0\right)\right)\right) \tag{2}$$

where N_{root} refers to the root node labelled by the failure event $HX1$. Each path, i.e. chain of events interconnecting through the BDD structure, linking the root node of the graph with a terminal 1 describes a system cut set and hence represents a possible failure mechanisms of the system.
One of the advantages associated with BDDs is the ease with which a tree can be converted to represent its complementary top event. This is represented by a Dual Binary Decision Diagram (DBDD), which can be easily obtained from the associated BDD by inverting the value of the terminal vertices while maintaining the structure unaltered. In terms of BDD structure, the result of the conversion procedure depends strongly on the variable ordering selected. In the current study, the conversion method developed by Rauzy [18] has been adopted applying the special ordering suggested by Sinnamon and Andrews [25]. According to this, FT gate events are considered in a top down ordering, with the only exception that at each gate the input basic events are listed with the repeated events first (if the gate has more than one repeated event as an input then the most repeated event is placed first).

2.5 Models Integration

BDDs encode Boolean functions through the combination of a graphical structure entailing edges, terminals and nodes, and the probabilistic information associated to these latter. The analysis of the graphical structure allows to define the possible combinations of events (or components states) resulting in the overall system failure, while the manipulation of the numerical information associated

to each node allows to quantify the likelihood of the failure. In light of this, the graphical layout of the BDD depends exclusively on the corresponding FT structure and the variable ordering adopted for the conversion, and hence is not affected by the nature of the events embraced and their probabilistic characterisation. However, in the proposed methodology the integration of the auxiliary PN and MM models discussed in Section 2.2 and 2.3, is still accomplished within the BDD definition, and more specifically by means of the numerical characterization of the nodes according to the nature of the event depicted.

As discussed so far, the probabilistic information associated with each basic FT event, and therefore with each BDD node, can be gathered from four possible sources:

- traditional maintenance models: referring to independent components or events characterised by constant failure and repair rates;
- marginal MM models: this option is available to model the life cycle of independent components characterised by constant failure/repair rate as well as complex maintenance strategies not captured by canonical maintenance models;
- marginal PN models: adopted to describe individual components characterised by non-exponentially distributed failure/repair times or by complex maintenance strategies (e.g. user-defined);
- joint MM models: used to model the interaction between failure mechanisms and repair processes of two or more components characterised by constant failure/repair rates;
- joint PN models: as for the former, this solution can be adopted to model the interdependencies and dynamic features existing between components, even when characterised by non-constant rates.

The first three categories result in the estimation of marginal unavailability values for independent components, and can therefore be associated with the corresponding nodes as for traditional BDDs, regardless of their origin (e.g. if MM/PN output or from traditional models). On the contrary, the computation of the joint PN and MM models results in the estimation of joint probabilities associated with each possible combination of outcomes of the dependent events included in a dependency group previously identify. Therefore, each BDD node belonging to a dependency group is associated with

a joint probability table covering all possible combinations of events entailed in the group rather than an individual probability value like in the other cases. Such tables are common to all nodes of the same dependency group and allow to integrate the output of the secondary PN and MM models within the BDD structure even when including component dependencies.
In light of this, the numerical characterisation of each BDD through the probabilistic output of PN and MM models (joint or marginal), represents the core of the multi-model integration on which the proposed methodology relies.

2.6 BDDs computation

The computational steps discussed so far provide a structure of independent BDDs as well as the reliability information associated with independent components and dependency groups. This information can now be processed in order to quantify each BDD, focusing on the prediction of three relevant reliability metrics: failure probability, failure frequency and component importance measures.
As discussed in the previous section, each path $PATH_i$ connecting a BDD root node with a terminal 1 represents a combination of components states leading to the failure of the system. In light of this, the failure probability of the system (i.e. the probability associated with the top event of the corresponding FT) can be calculated as the sum of the probability values associated with each such path. This can be expressed as:

$$Q_{system} = \sum_{i=1}^{m} q(PATH_i) \tag{3}$$

where $q(PATH_i)$ indicates the probability associated with the $i-th$ of the m disjoint paths connecting the BDD root to a terminal 1.
In order to achieve an adequate understanding of a system's behaviour, it is desirable to measure the contribution of individual components to its overall failure probability. This can be estimated for a generic component X as the difference of the system failure probability assuming the component X_j has failed (i.e. $Q_{system}(X_j)$), minus the system failure probability assuming the component to work correctly (i.e. $Q_{system}(\overline{X_j})$). This quantity is known as the Birnbaum's measure of importance of

the component, and can be expressed as:

$$G(X_j) = \frac{\partial Q_{system}}{\partial q(X_j)} = Q_{system}(X_j) - Q_{system}(\overline{X_j}) \tag{4}$$

The third metrics of interest in this study can be finally computed from the Birnbaum's measure of importance for the components as:

$$F_{system} = \sum_{j=1}^{k} G(X_j) \cdot f(X_j) \tag{5}$$

where $f(X_j)$ refers to the failure intensity of the $j-th$ of the k components of the system, and F_{system} is the overall failure intensity.

If the BDD refers to an independent subsystem, and hence matches one of the subsystem FTs in the input, the reliability information obtained is directly relevant to the independent subsystem itself. Conversely, if the BDD results from the creation of a merged FT due to the existence of dependencies between two or more subsystems (as discussed in Section 3.4, the reliability information refers to the joint state of the two subsystems. For instance, with reference to the example of Fig.6, the quantification of the BDD obtained from the conversion of the merged FT will result in the probability associated with the top event indicating the simultaneous failure of both subsystems.

Finally, the occurrence of one or more dependency groups within a FT implies the presence of components dependencies in the resulting BDD. Currently available algorithms for the computation of BDDs do not allow for stochastic dependencies, relying instead on the assumption of components independence typical of FT analysis. In light of this, the simulation framework proposed required the development of novel solutions for the quantification of BDDs in the presence of dependencies. The approach adopted relies on the calculation of the probability of all BDD paths to failure using independent and joint probabilities, as well as their manipulation, as appropriate. This strategy has been implemented in a novel algorithm [29] and integrated in the simulation framework presented.

2.7 ET computation

The computation of the independent BDDs provides the information necessary to complete the safety analysis, through the calculation of the overall system ET. If the subsystems defining the ET branches are all mutually independent, the computed BDDs match the input FTs structure and hence refer to individual subsystems: in this case the computation of the ET is straightforward, utilising the initiating event failure intensity and of the probability of failure of the remaining subsystems. If instead two or more subsystems included in the ET are linked by some sort of dependency, the computation of the ET requires the use of conditional, rather than marginal, probabilities. This can be easily gathered from the joint probabilities calculated from the merged BDD (as discussed in Section 2.4 and 2.6) according to the marginalisation and conditioning rules. The first of this can be applied in order to extrapolate marginal values of probability from joint estimates, as:

$$q(X_i) = \sum_{\mathbf{X_j}} q(\mathbf{X_i} = X_i, \mathbf{X_j}) \tag{6}$$

where the marginal value $q(X_i)$ was obtained summing over the set of probability values $q(\mathbf{X_i} = X_i, \mathbf{X_j})$ obtained from BDDs analysis and associated with the occurrence of state X_i regardless of the state of dependent component X_j. Similarly, the conditional probability of component X_j to be in its failed state given the failure of X_i can be computed as:

$$q(X_j \mid X_i) = \frac{q(X_i, X_j)}{q(X_i)} \tag{7}$$

3 Numerical Application

To demonstrate the methodology and explore the effects of different assumptions in the analysis, the proposed approach has been applied to five simple case-studies characterised by different degrees of complexity:

1. Case Study A: relies on conventional assumptions such as full independence with no component

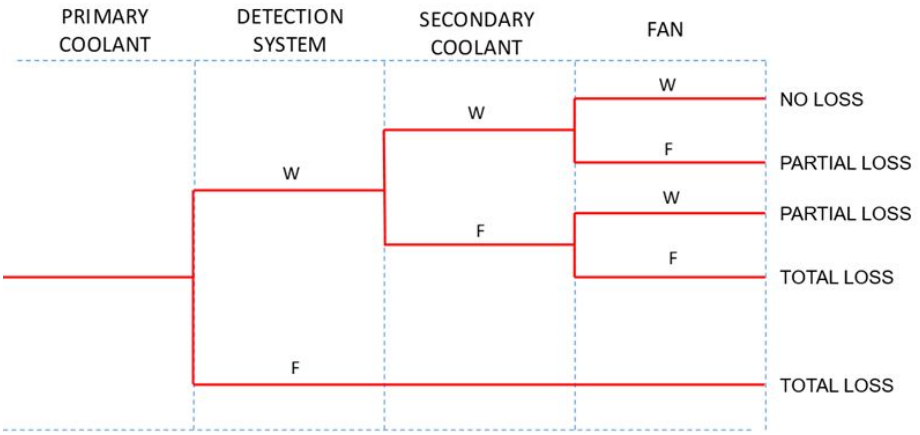


Figure 7: Event tree for the model in Section 3

degradation.

2. Case Study B: investigates the inclusion of component degradation in the analysis while maintaining the assumption of independence.

3. Case Study C: focuses on dependencies resulting from shared basic events between two or more subsystems. This is referred as a 'hard' dependency.

4. Case Study D: investigates a category of dependencies referred to as 'soft'. These include dependencies triggered by secondary procedures or processes, which may be not strictly connected with the hardware function (e.g. maintenance, load, surrounding conditions etc.).

5. Case Study E: considers the overlapping of the dependency types investigated in Case C and D. This is referred to as a 'complex' dependency.

The following sections provide a detailed description of the analysis carried out for each case listed above. All case studies refer to the same system design, whose detail are provided in the following section.

3.1 System Model

A simplified power plant cooling system has been selected for testing the proposed methodology. The system design is shown in Fig.8 and embraces four subsystems:

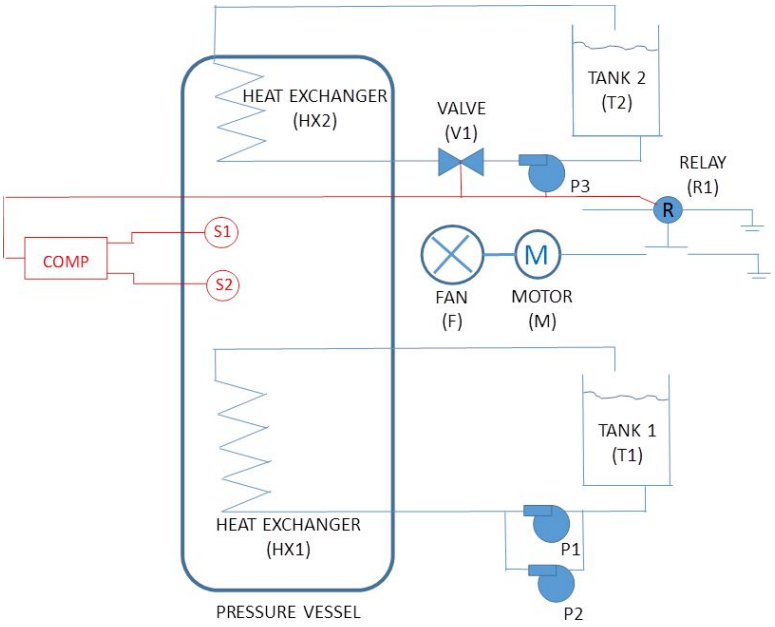
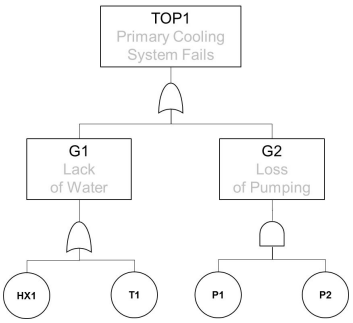


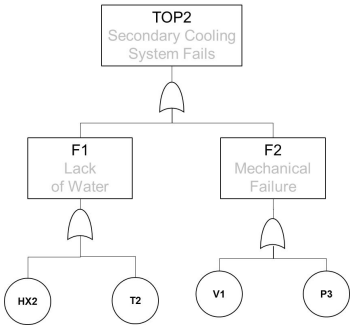
Figure 8: System model for demonstration of concepts

- Primary Cooling System: this consists of a heat exchanger $HX1$ which is fed cooling water from a storage tank $T1$. The circulation is ensured by the operation of two identical pumps working in parallel, $P1$ and $P2$ (both normally operational). The failure of either $HX1$ or $T1$ prevents the correct functioning of the primary cooling system. Similarly, the simultaneous unavailability of the circulation pumps $P1$ and $P2$ leads to the overall failure of the subsystem. Conversely, the failure of only one of the two pumps, does not affect the operation of the primary cooling system since both pumps have the capability to provide the coolant required. The FT summarising the possible failure mechanisms of the primary cooling system is shown in Fig. 9a.

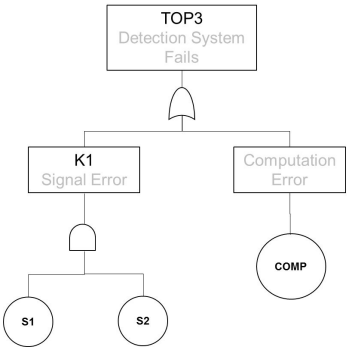
- Secondary Cooling System: it partially provides the required vessel cooling capability. Similarly to the primary cooling, it comprises a heat exchanger $HX2$, a storage tank $T2$ and a pump $P3$ responsible for the circulation of cooling water. Additionally, the valve $V1$ opens to allow water to flow only when the primary system has failed and $P3$ is activated and working correctly. The failure of any of the mentioned components prevents the correct operation of the system, as shown by the FT in Fig. 9b, resulting in the unavailability of secondary cooling.



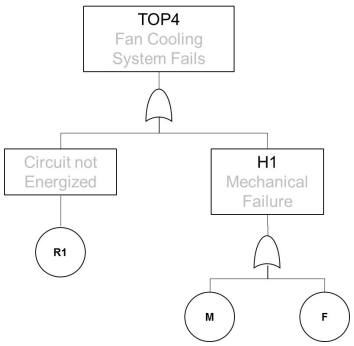
(a) FT for the primary cooling subsystem



(b) FT for the secondary cooling subsystem



(c) FT for the detection subsystem



(d) FT for the fan cooling subsystem

Figure 9: BDD structures for subsystems

- Detection System: the temperature within the vessel is expected to rise in the case of failure of the primary cooling system. By design, such increase is detected by dedicated sensors, $S1$ and $S2$, working in parallel and transmitting the reading to a programmable logic controller $COMP$. When the temperature readings from $S1$ and $S2$ exceed a pre-established threshold, the controller activates both the secondary and fan cooling systems. The failure of the subsystem controller results in the unavailability of the entire system, as shown by the FT of Fig. 9c. On the contrary, the failure of only one of the two sensors does not affect the correct operation of the subsystem.

- Fan System: like the secondary cooling system, the fan has the capability to provide partial cooling of the vessel. When relay $R1$ energises and its contacts close, the associated circuit

activates the electric motor M operating fan (F). The failure of any of these components results in the unavailability of the subsystem, as highlighted by the FT in Fig. 9d.

Any combination of subsystems states has the potential to result in different consequences, as summarised by the ET in Fig. 7. The failure of the primary cooling system can result in the total loss of cooling only if in combination with the failure of the detection system (preventing the activation of secondary mitigation measures) or in the case of simultaneous loss of the secondary and fan cooling systems. Conversely, if one of the latter two subsystems operates correctly but not the other, there will be a partial cooling loss. Finally, if all but the primary cooling subsystem are available, no cooling loss is registered.

3.2 Case A

This is the simplest case considered, relying on the assumption of full independence and neglecting any degradation process to which the components may be subject. In light of this, the reliability metrics of the components can be calculated according to conventional failure models, as discussed in Section 2.2.

For a component X whose failure immediately apparent and for which corrective action is in place (e.g. revealed failure), the unavailability $q(X)$ can be expressed as:

$$q(X) = \frac{\lambda}{\lambda + \nu} \tag{8}$$

where λ and ν represent the component's failure and repair rates respectively. This is the case for all the components belonging to the primary system, since their failure would directly affect the performance of the system. On the other hand, the malfunctioning of components belonging to the secondary, detection and fan systems, might be not detected on occurrence due to the subsystems not being continuously operational (i.e. unrevealed failure). Scheduled maintenance with regular inspections is assumed to be in place for such components, whose unavailability can hence be calculated as:

$$q(X) = \lambda \cdot (\frac{\theta}{2} + \frac{1}{\nu}) \tag{9}$$

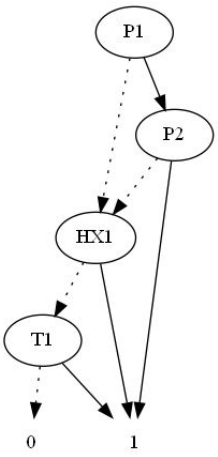
COMPONENT	FAILURE RATE $[h^{-1}]$	MTTR $[h]$	UNAVAILABILITY	FAILURE INTENSITY
HX1	$1.7e^{-06}$	24	$4.08e^{-05}$	$1.70e^{-06}$
T1	$2.7e^{-08}$	8	$2.16e^{-07}$	$2.70e^{-08}$
P1	$8.0e^{-04}$	8	$6.40e^{-03}$	$7.95e^{-04}$
P2	$8.0e^{-04}$	8	$6.40e^{-03}$	$7.95e^{-04}$
HX2	$1.7e^{-06}$	14	$3.72e^{-03}$	$1.69e^{-06}$
T2	$2.7e^{-08}$	260	$5.91e^{-05}$	$2.69e^{-08}$
V1	$2.7e^{-07}$	5	$5.91e^{-04}$	$2.69e^{-07}$
P3	$8.0e^{-04}$	8	$1.09e^{-03}$	$4.99e^{-07}$
S1	$1.7e^{-06}$	3	$3.72e^{-03}$	$1.69e^{-06}$
S2	$1.7e^{-06}$	3	$3.72e^{-03}$	$1.69e^{-06}$
COMP	$3.1e^{-06}$	12	$6.70e^{-03}$	$3.04e^{-06}$
R1	$3.4e^{-07}$	3	$7.44e^{-04}$	$3.40e^{-07}$
M	$8.0e^{-06}$	150	$4.38e^{-03}$	$1.99e^{-06}$
F	$3.5e^{-06}$	40.5	$7.66e^{-03}$	$3.47e^{-06}$

Table 1: Components failure reliability information for case-study A

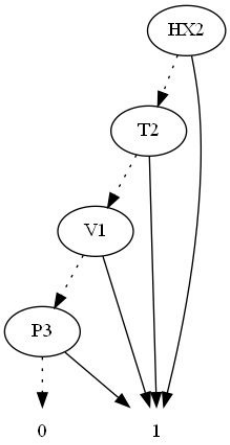
where θ refers to the time interval between inspections. The failure intensity $f(X)$ can be then calculated for the generic component X as:

$$f(X) = \lambda(1 - q(X)) \tag{10}$$

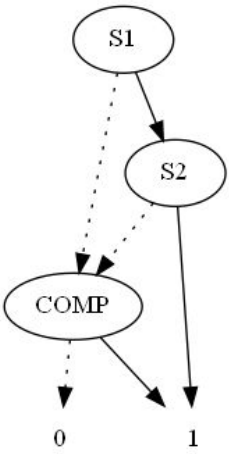
The components reliability information and the relative metrics calculated according to the above equations are shown in Table 1. A regular time interval of 4380 h between inspections, corresponding to a six monthly maintenance schedule, has been assumed for all components except those belonging to the primary cooling system. According to the procedure discussed in Section 2, the next step in the methodology focuses on the identification and computation of dependency groups. However, this does not apply in the current case since all components and subsystems are assumed independent. Subsequently, the FTs shown in fig.9a - 9d are independent and can be converted to BDD structures as discussed in Section 2.4. The resulting BDDs are shown in Fig.10, where dashed lines indicate 0 branches, continuous lines refer to 1 branches. Once the structure of the BDDs has been generated, their numerical analysis is carried out as discussed in Section 2.6. The resulting failure probability values associated to each subsystem are shown in Table 2. The subsystems FTs were also analysed



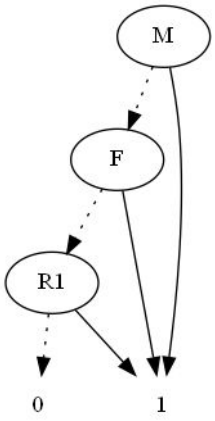
(a) Primary cooling system BDD



(b) Secondary cooling system BDD



(c) Detection system



(d) Fan cooling system BDD

Figure 10: BDD structures for subsystems

adopting the Minimal Cut Set Upper Bound approximation [2] [1], in order to verify the algorithms implemented.

As shown in Fig.7, the failure of the primary cooling system works as trigger event for the overall system failure. For this reason the failure frequency associated with the primary system was computed, resulting in $1.1901e^{-05}\ h^{-1}$. From this and the subsystems failure probabilities previously calculated, it is finally possible to estimate the system ET outcome frequencies for the possible degrees of cooling loss. The results obtained are shown in Table 7.

SUBSYSTEM	FAILURE PROBABILITY
$PRIMARY$	$8.1942e^{-05}$
$SECONDARY$	$5.4615e^{-03}$
$DETECTION$	$6.7154e^{-03}$
FAN	$1.2747e^{-02}$

Table 2: Subsystems failure probability for case-study A

3.3 Case B

Assume the components $HX1$ and $T1$ from the primary cooling system to be characterised by a non-constant failure rate, and their failure time follows a Weibull distribution. In addition to this, let assume $T1$ to be characterised by a lognormal repair time distribution.

As described in Section 2.2, the proposed approach relies on the use of PNs to compute the reliability of components characterised by non-constant failure or repair rates. The lifecycle of $T1$ is then simulated running to convergence the PN shown in Fig.3, computing then the component unavailability as the ratio between the total simulated downtown over the overall simulated life. An identical PN structure has been adopted for $HX1$. Specifics of the distributions adopted in the current case-study and the resulting reliability metrics are provided in Table 3. Substituting such values into the analysis of the primary subsystem BDD (to which the components under study belong), the associated failure probability $q(PRIMARY)$ and intensity $f(PRIMARY)$ are:

$$q(PRIMARY) = 9.230e^{-03} \tag{11}$$

$$f(PRIMARY) = 1.2257e^{-05}h^{-1} \tag{12}$$

Also in this case the computation of the system ET is conventional, thanks to the assumption of full independence. Table 7 shows the results obtained updating the ET calculation in view of the new probability and intensity values for the primary system failure in Eq.11.

3.4 Case C

Consider now the situation where pump $P2$ is common to both the primary and secondary cooling systems (see Fig. 9b). As such, $P2$ replaces $P3$ in the FT representing the failure of the secondary

COMPONENT	FAILURE TIME [h]	REPAIR TIME [h]	UNAVAILABILITY	FAILURE FREQUENCY
HX1	Weibull [3, 6622.7]	Exponential [0.0417]	$3.92e^{-3}$	$1.70e^{-06}$
T1	Weibull [2, 417920]	Lognormal [8, 4.125]	$5.29e^{-3}$	$4.87e^{-7}$

Table 3: Assumptions for case-study B

subsystem. To model the real setting of the system, it is now necessary to take into account the dependency triggered by the shared component $P2$ and linking the primary and secondary cooling system FTs. As discussed in Section 2.4, this is achieved merging the dependent FTs, computing the resulting BDDs, and extracting from the analysis the joint probability associated with all the possible combinations of states of the two subsystems. In this case, only combinations of states including the failure of the primary cooling system are of relevance for the safety analysis, since the working state of the primary cooling would instead garantee the correct operation of the overall system (see Fig.7). Hence, the probability estimates of interest are:

- $q\left(PRIMARY, SECONDARY\right)$: probability of simultaneous failure of the primary and secondary cooling;
- $q\left(PRIMARY, \overline{SECONDARY}\right)$: probability of the failure of the primary cooling but the correct operation of the secondary cooling.

The first of these is estimated from the analysis of the FT obtained merging (ANDing) the two subsystem FTs, as shown in Fig. 6. Similarly, the probability $q\left(PRIMARY, \overline{SECONDARY}\right)$ can be calculated as the top event of a FT obtained merging the primary cooling FT in input with the working state (dual) model of the secondary cooling system FT initially provided. The resulting tree is shown in Fig.11. Having defined the FTs of interested, they are converted to BDDs, giving the structures shown in Fig.12. Since the dependency considered in this case is caused by the repetition of the component $P2$ in two subsystems, the merging of the FTs is sufficient to guarantee the validity of the independence assumptions and the resulting BDDs can be computed using traditional algorithms. The results of the BDDs analysis are shown in Table 4: while the probability associated with the failure of the detection and fan subsystem remain unchanged (the parameters for these

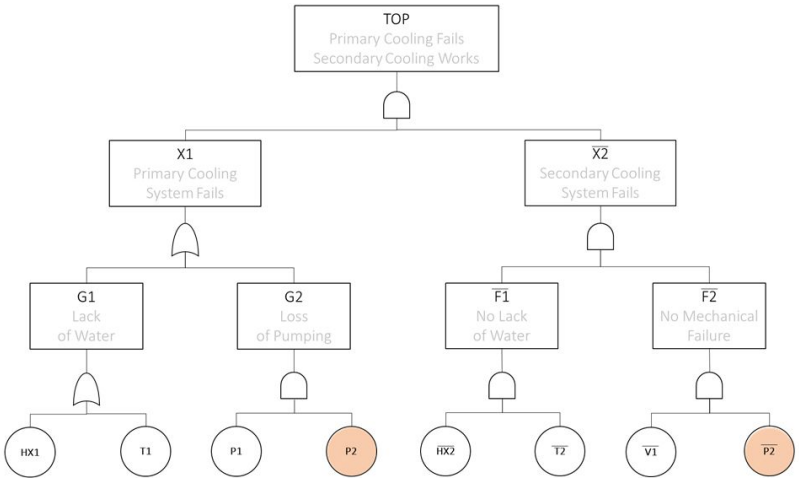
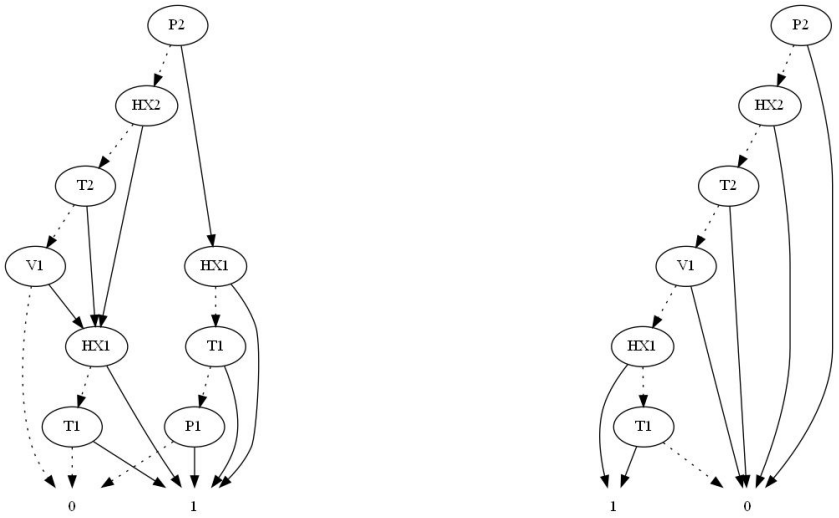


Figure 11: Merged FT for case B. Repeated components are highlighted

SUBSYSTEM	**FAILURE PROBABILITY**
$PRIMARY\&SECONDARY$	$4.1399e^{-05}$
$PRIMARY\&\overline{SECONDARY}$	$8.1942e^{-05}$
$DETECTION$	$6.7154e^{-03}$
FAN	$1.2747e^{-02}$

Table 4: Subsystems failure probability for case-study C



(a) BDD of the joint FT in Fig. 6 (b) BDD of the joint FT in Fig. 11

Figure 12: BDDs for relevant combination of states of primary and secondary system

systems are identical in cases A, B and C), joint values are provided for the primary and secondary cooling.

As discussed in Section 2.7, the system ET can be now computed taking into account the dependencies underlying the two systems and manipulating the relative joint probability. For instance, the frequency associated with the consequence $NOLOSS$, can be now calculated as:

$$f(NOLOSS) = f(PRIMARY) \cdot q(\overline{DETECTION}) \cdot q(\overline{SECONDARY}|PRIMARY) \cdot q(\overline{FAN}) \quad (13)$$

where $q(\overline{SECONDARY}|PRIMARY)$ refers to the probability of the secondary system to work given that the primary coolant system has failed, and $f(PRIMARY)$ to the failure frequency of the primary coolant subsystem. This can be calculated according to the conditioning procedure shown in Eq.7, resulting in:

$$q(\overline{SECONDARY}|PRIMARY) = \frac{q(PRIMARY, \overline{SECONDARY})}{q(PRIMARY)} \quad (14)$$

where $q(PRIMARY)$ can in turn be estimated through marginalisation (see Eq.6) as:

$$q(PRIMARY) = q(PRIMARY, \overline{SECONDARY}) + q(PRIMARY, SECONDARY) \quad (15)$$

using the joint probability values $q(PRIMARY, \overline{SECONDARY})$ and $q(PRIMARY, SECONDARY)$ obtained from the the BDD analysis. Similarly, the probability of the secondary cooling to fail given the failure of the primary system can be obtained as:

$$q(SECONDARY|PRIMARY) = \frac{q(PRIMARY, SECONDARY)}{q(PRIMARY)} \quad (16)$$

In light of this, the computation of the system ET can be completed, resulting in the loss frequency values shown in Table 7.

3.5 Case D

In the system, the circulation of cooling water within the primary subsystem is ensured by the operation of two identical pumps working in parallel, namely P1 and P2. Let now account for the fact that the failure of one pump will require the second pump to deliver the full supply and therefore be subject to a higher load, increasing its probability of failure. Such a relationship between the two components is modelled by the PN shown in Fig.4 as well as by the MM shown in Fig.5. Assuming the repair and failure times of both pumps to be exponentially distributed, the steady-state solution can be easily calculated for the associated MM, to gain advantages in terms of computational time. The two components are assumed to be subject to corrective maintenance with the same repair rate used in the previous cases, as well as the same failure rate when under design load. However, the failure rates of the two components increase when the pump is subject to a higher load (i.e. when the other pump is out of order). Adopting the parameters shown in Table 6, the steady-state solution of the MM leads to the joint values shown in Table 5: as expected, the joint unavailability of $P1$ and $P2$ results to be one order of magnitude higher than the product of their unavailability calculated assuming independence.

Carrying out the analysis of the BDD associated with the primary cooling using the joint values

STATE	PROBABILITY	FREQUENCY
$P1, P2$	$1.3362e^{-04}$	$3.3406e^{-05}$
$P1, \overline{P2}$	$6.1863e^{-03}$	$7.8999e^{-04}$
$\overline{P1}, P2$	$6.1863e^{-03}$	$7.8999e^{-04}$
$\overline{P1}, \overline{P2}$	$9.8749e^{-01}$	$1.5799e^{-03}$

Table 5: Output of the MM in Fig. 5

PARAMETER	VALUE
$\lambda 1$	$8.00e^{-04}$
$\lambda 2$	$2.70e^{-03}$
ν	$1.25e^{-01}$

Table 6: Input of the MM in Fig. 5

obtained, the probability of the subsystem to fail results equal to $1.7460e^{-04}$ which is more than two times higher the estimate of case A. The probability values associated with the failure of the remaining subsystems remain instead unchanged (see Table 2). The analysis of the ET results in the loss frequency provided in Table 7. The obtained frequencies show the impact of the $P1$ and $P2$ dependency on the overall safety of the system: both the values associated with partial and total loss of cooling result to be higher than what computed in case of independence.

3.6 Case E

Engineering systems can be characterised by complex dependency structures, not easily attributable to a single type as for the examples above. In order to test the proposed approach against a similar case, case-studies C and D have been merged into one: let P2 be shared by the primary and secondary cooling systems, as well as being dependent on P1. The resulting BDD structures are then identical to those shown in Fig.12. However, as for case D, their computation requires the use of the joint probability associated with the failure and operation of both primary and secondary

LOSS	CASE A $[h^{-1}]$	CASE B $[h^{-1}]$	CASE C $[h^{-1}]$	CASE D $[h^{-1}]$	CASE E $[h^{-1}]$
NONE	$1.1606e^{-05}$	$1.1954e^{-05}$	$1.4415e^{-05}$	$3.5639e^{-05}$	$3.9613e^{-05}$
PARTIAL	$2.1360e^{-07}$	$2.1999e^{-07}$	$7.4687e^{-06}$	$6.5588e^{-07}$	$3.0926e^{-05}$
TOTAL	$8.0742e^{-08}$	$8.3158e^{-08}$	$2.4262e^{-07}$	$2.4793e^{-07}$	$8.7226e^{-07}$

Table 7: Loss frequencies for the case studies analysed

cooling subsystem (see Table 5). Therefore case E contemplates the stochastic dependency between P1 and P2, where P2 is a component of both the primary and secondary cooling subsystems. The quantification of the failure probability of these latter, allows to estimate the effect of such system setting in terms of system reliability. Indeed, as shown in Table 8, the probability of a simultaneous failure of both subsystems is equal to $1.3405e^{-04}$, which is over 3 times higher than the estimate obtained in case C (i.e. considering the stochastic dependency between the two pumps but assuming P3 to service the secondary cooling instead of P2). However, when compared to the system setting entailing only stochastic dependency (case D), the gap between values widens considerably, with the joint probability of the primary and secondary system to fail being 3 order of magnitude higher than its value assuming independence. Therefore, both the stochastic dependency between P1 and P2 and the dependency between the two cooling subsystems (due to the shared use of P2) rise individually the likelihood of a simultaneous failure of the primary and secondary cooling, with the second giving the highest contribution to the increase. This is due to the decline of system redundancy triggered by the substitution of P3 (as in case D) with P2. On the other hand, the probability associated with the failure of the primary subsystem and the correct operation of the secondary cooling decreases when considering the stochastic dependency between the two parallel pumps P1 and P2: the estimate indeed results to be only 20% of the value calculated in case C, assuming components independence. This suggests that, when considering the components dependency, the failure of the primary system is more likely to occur in combination with the failure of the secondary cooling rather than along its working state. This reflects on the overall system loss frequencies: as shown in Table 7, the frequency values for the current case are the highest across all system setting considered as well as losses type. This is true also when considering the occurrence of no cooling losses for which, involving the working of the secondary system, a lower frequency value could be expected for case E in comparison with case D, due to the difference in the relative joint probabilities. However, the gap between the failure probabilities discussed before is mitigated, and its effect on the overall loss frequency reverted, by the increased frequency for the primary cooling failure registered when considering the stochastic dependency between P1 and P2.

SUBSYSTEM	FAILURE PROBABILITY
$PRIMARY\&SECONDARY$	$1.3405e^{-04}$
$PRIMARY\&\overline{SECONDARY}$	$1.7459e^{-05}$
$DETECTION$	$6.7154e^{-03}$
FAN	$1.2747e^{-02}$

Table 8: Subsystems failure probability for case-study E

4 Accuracy and Scalability

The strength of the proposed methodology lies with the capability of isolating aspects of the system behaviour which defy conventional FT/ET analysis assumptions, modelling them with more detailed and flexible strategies such as MMs and PNs. This is achieved integrating the initial FT models and the MM/PN output within the BDD frameworks, thanks to the development of algorithms for the computation of these latter taking into account dependencies. Of course, while hopefully paving the path towards more realistic and accurate modelling, this kind of approach opens the doors to new challenges associated with the nature of the newly available modelling capability and their computational cost, such as:

- The use of BDD with dependencies, which comes at the cost of higher computational power. The magnitude of such an increase depends on the model structure. As a limited term of comparison, the computation of case A in the current study was carried out in 0.01 s, while the analysis of case E employed 0.03 s. To mitigate the costs associated with real-world systems and ensure the scalability of the approach, the size of the model sections entailing dependencies can be reduced, hence minimizing the use of more expensive algorithms associated with their computation. This can be achieved through modularisation, currently under implementation, consisting in reducing the initial FT structure [14], and subsequentially extracting independent sections of the tree circumscribing the dependent components [11] [27]. Such sub-models can be then analysed separately with the novel approach for the computation of BDD in presence of dependencies, and the results re-introduced in the initial FT model in the form of an independent surrogate event retaining reliability information equivalent to the section analysed. The FT so modified could be then analysed with traditional approaches, whose feasibility for large scale systems has been largely proved.

- The computational burden of stochastic models and simulation techniques, such as PNs and MMs, increases significantly with model size or when rare events are involved. As for the case above, this can be mitigated minimizing the model size. In light of this, an unconventional PN modelling strategy has been implemented in the proposed framework. This technique inherits the main aspects of traditional PNs but allows to record the joint state of the places of interest in the network whenever a transition is fired, giving directly as output joint probabilities and frequencies and hence avoiding the use of places representing the joint state under study. In the case of n dependent and Boolean components, the associated PN model would require $2 \cdot n + 2^n$ places, while the alternative PN solution reduces such number to $2 \cdot n$. With regards to the PN network in Fig.4, this would translate in the computation of only the red section of the model, with advantages in terms of efficiency and without affecting the accuracy of the analysis. Other possible strategies to enhance the efficiency of the simulations would entail the use of advanced Monte Carlo sampling techniques [7] [28].

- The proposed approach removes simplifying assumptions and limitations associated with traditional FT analysis, providing analysts with a higher degree of flexibility but also transferring to them the task of identifying modelling assumptions. Indeed, while the FT construction process would remain unvaried, the proposed framework allows to specify further the relationship between components. This implies firstly the need to identify relevant dependencies or complex relationships between components. The first of these two tasks should be addressed on the basis not only of the meticulous knowledge of the system (as for FT analysis), but also of the nature of the interaction between components. Indeed, the model implementation should be preceded by an analysis of component dependencies, which could be carried out systematically on the basis of the different source of dependency, e.g. causal dependencies (when the state of a component directly affects the probability of failure of another component), maintenance strategies, common environmental factors etc. Once identified possible dependency relationships between components, the further step is to estimate their relevancy. Such task is not banal, since any direct numerical estimation of the dependency relevancy would have to rely on the comparison of the joint and marginal probabilities of the interested components, hence implying the modelling of the dependency relationship. While the possible exclusion of the

investigated dependency from the model due to lack of significance would decrease the computational burden of the analysis, it would not reduce the modelling load for the analyst, due to the necessity to estimate the joint probabilities. Further support for the decision making process could be provided by importance measures, allowing for example to exclude complex feature modelling when this entail low importance components. Ultimately, the identification of complex features to include in the modelling would be mostly dictated by the expertise and knowledge of the system: while this may increase the complexity of the modelling process, it would also push towards a better understanding of the system as an interconnected network of components, forcing the analyst to consider aspects of the system which would be left implicitly hidden when adopting more traditional techniques.

- Aside from determining which complex feature to consider in the analysis, the new modelling capability requires also to explicitly decide the degree of detail of the more sophisticated model sections (e.g. PN and MM). This would partly depend on the data availability, but mostly leads back to the long-standing issue of finding a balance between model accuracy and its costs. Also in this case the strength of the model and its robustness could be evaluated through numerical strategies, such as sensitivity analysis, but would still increase the modelling burden. However, as for the previous point, it is worth to highlight that the need to explicitly identify these analysis details is in itself a significant achievement, even if not without challenges. Indeed, the new capabilities allow to reduce (if not eliminate) implicit assumptions of traditional techniques, returning to the analyst a realistic picture of the complexity of the systems under study and providing the basis for a better understanding, and potentially representation, of complex systems.

5 Conclusions

The research presented proposes a novel methodology aiming to overcome the limitations of traditional fault and event tree techniques, whilst preserving their familiar modelling formulation as well as their computational efficiency. This is achieved through a surgical approach to modelling, relying on the identification of minimal model subsets requiring a degree of simulation fidelity beyond the

capability of traditional methodologies (e.g. dependencies, degradation processes, complex maintenance strategies etc.) and their resolution through the use of Petri nets and Markov models. On the one hand, the use of the latter ensures extreme modelling flexibility and promotes the shifts towards more realistic modelling. On the other, the restriction in the use of these more expensive modelling solutions to only the sections of the system for which traditional simplifying assumptions (e.g. components independence, failure rate constancy) are unjustified, ensures the computational feasibility and scalability of the approach. The methodology developed is tested against five case-studies, covering a range of component dependency types and system settings which cannot be fully represented through the use of conventional fault and event trees. The results obtained are compared to those achieved with existing techniques, in order to verify the accuracy as well as the computational efficiency of the implemented algorithms.

Acknowledgment

This work was supported by the Lloyd's Register Foundation, a charitable foundation in the U.K. helping to protect life and property by supporting engineering-related education, public engagement, and the application of research.

References

[1] J. D. Andrews and S. J. Dunnett. Event-tree analysis using binary decision diagrams. *IEEE Transactions on Reliability*, 49(2):230–238, 2000.

[2] J. D. Andrews and T. R. Moss. *Reliability and risk assessment.* Professional Engineering Publishing, 2002.

[3] A. Bobbio. System modelling with petri nets. In *Systems reliability assessment*, pages 103–143. Springer, 1990.

[4] C. Bonivento, M. Capiluppi, L. Marconi, A. Paoli, and C. Rossi. Reliability evaluation for fault diagnosis in complex systems. In *Fault Detection, Supervision and Safety of Technical Processes 2006*, pages 1330–1335. Elsevier, 2007.

[5] M. Bouissou and J.-L. Bon. A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes. *Reliability Engineering & System Safety*, 82(2):149–163, 2003.

[6] D. Braha, N. Suh, S. Eppinger, M. Caramanis, and D. Frey. Complex engineered systems. In *Unifying Themes in Complex Systems*, pages 227–274. Springer, 2006.

[7] O. Cappé, S. J. Godsill, and E. Moulines. An overview of existing methods and recent advances in sequential monte carlo. *Proceedings of the IEEE*, 95(5):899–924, 2007.

[8] M. Čepin and B. Mavko. A dynamic fault tree. *Reliability Engineering & System Safety*, 75(1):83–91, 2002.

[9] R. Drechsler and B. Becker. *Binary decision diagrams: theory and implementation.* Springer Science & Business Media, 2013.

[10] J. B. Dugan, S. J. Bavuso, and M. A. Boyd. Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Transactions on reliability*, 41(3):363–377, 1992.

[11] Y. Dutuit and A. Rauzy. A linear-time algorithm to find modules of fault trees. *IEEE Transactions on Reliability*, 45(3):422–425, 1996.

[12] P. A. Gagniuc. *Markov chains: from theory to implementation and experimentation.* John Wiley & Sons, 2017.

[13] J. K. Muppala, M. Malhotra, and K. S. Trivedi. Markov dependability models of complex systems: Analysis techniques. In *Reliability and Maintenance of Complex Systems*, pages 442–486. Springer, 1996.

[14] O. Platz and J. V. Olsen. *FAUNET: A program package for evalution of fault trees and networks.* Risø National Laboratory, 1976.

[15] S. J. Prowell. Using markov chain usage models to test complex systems. In *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, pages 318c–318c. IEEE, 2005.

[16] J. Pukite and P. Pukite. *Modeling for reliability analysis: Markov modeling for reliability, maintainability, safety, and supportability analyses of complex systems.* John Wiley & Sons, 1998.

[17] K. D. Rao, V. Gopika, V. S. Rao, H. Kushwaha, A. K. Verma, and A. Srividya. Dynamic fault tree analysis using monte carlo simulation in probabilistic safety assessment. *Reliability Engineering & System Safety*, 94(4):872–883, 2009.

[18] A. Rauzy. New algorithms for fault trees analysis. *Reliability Engineering & System Safety*, 40(3):203–211, 1993.

[19] A. Rauzy. Binary decision diagrams for reliability studies. In *Handbook of performability engineering*, pages 381–396. Springer, 2008.

[20] W. Reisig. *Petri nets: an introduction*, volume 4. Springer Science & Business Media, 2012.

[21] R. Y. Rubinstein and D. P. Kroese. *Simulation and the Monte Carlo method*, volume 10. John Wiley & Sons, 2016.

[22] E. Ruijters and M. Stoelinga. Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools. *Computer science review*, 15:29–62, 2015.

[23] S. A. Sheard and A. Mostashari. Principles of complex systems for systems engineering. *Systems Engineering*, 12(4):295–311, 2009.

[24] F. Sihombing and M. Torbol. Parallel fault tree analysis for accurate reliability of complex systems. *Structural Safety*, 72:41–53, 2018.

[25] R. M. Sinnamon and J. Andrews. Improved accuracy in quantitative fault tree analysis. *Quality and reliability engineering international*, 13(5):285–292, 1997.

[26] R. M. Sinnamon and J. Andrews. New approaches to evaluating fault trees. *Reliability Engineering & System Safety*, 58(2):89–96, 1997.

[27] H. Sun and J. D. Andrews. Identification of independent modules in fault trees which contain dependent basic events. *Reliability Engineering & System Safety*, 86(3):285–296, 2004.

[28] S. T. Tokdar and R. E. Kass. Importance sampling: a review. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(1):54–60, 2010.

[29] S. Tolo and J. Andrews. Fault Tree analysis including component dependencies. *Currently Under Review*.

[30] M. Volk, S. Junges, and J.-P. Katoen. Fast dynamic fault tree analysis by model checking techniques. *IEEE Transactions on Industrial Informatics*, 14(1):370–379, 2017.

[31] M. Walker, L. Bottaci, and Y. Papadopoulos. Compositional temporal fault tree analysis. In *International Conference on Computer Safety, Reliability, and Security*, pages 106–119. Springer, 2007.

[32] H. Xu and J. B. Dugan. Combining dynamic fault trees and event trees for probabilistic risk assessment. In *Annual Symposium Reliability and Maintainability, 2004-RAMS*, pages 214–219. IEEE, 2004.