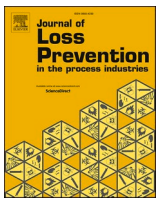
Journal of Loss Prevention in the Process Industries 94 (2025) 105545

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp



Extending the dynamic and dependent tree theory (D^2T^2) to safety barriers: An application to an offshore fire deluge system

Leonardo Leoni [a], John Andrews [b], Filippo De Carlo [a,*]

[a] Department of Industrial Engineering (DIEF), University of Florence, Italy
[b] Faculty of Engineering, University of Nottingham, United Kingdom

ARTICLE INFO

Keywords:
Fault tree analysis
Dependency modelling
Petri net
Markov chain
Water deluge system

ABSTRACT

Fault Tree (FT) Analysis is still one of the most common approaches for conducting reliability analysis of complex systems. However, it conceals several limitations such as the assumption of independent events and inability to model modern maintenance strategies in its basic form. To enhance FT analysis and overcome these limitations, Dynamic and Dependent Tree Theory, D^2T^2, has been recently introduced. This algorithm is based on the integration of Petri Nets, Markov models, and Binary Decision Diagram with the FT. Despite its effectiveness, its generalizability for different case studies needs to be explored. This is especially true for the application to safety barriers, which spend most of their time in a standby state. Thus, this paper aims to provide an extension of the D^2T^2 approach to further prove its capabilities and adopt it for safety barriers. To this end, the framework is applied to an offshore fire deluge system considering an availability analysis and a reliability analysis for the standby and operational phase respectively. The proposed modified framework could be used by maintenance engineers and managers to conduct reliability analysis of safety barriers, along with testing multiple maintenance strategies for their components.

1. Introduction

Fault Tree Analysis (FTA) is a very prominent technique used for reliability and risk analyses and avoid losses. A FT is a graphical method, which represents how the causes for an undesired top event could be generated: the leaves represent component failures, while the gates represent how the failures propagate (Ruijters and Stoelinga, 2015). FTA is both qualitative and quantitative. Generally, the first stage of a FTA would be qualitative since it requires to define the logic behind the system failure generation. Next, the second stage would be estimating the probability or frequency of the top event, possibly evaluating also some important measures (Andrews, 2002). The importance of FTA has progressively increased, leading to a widespread adoption in different fields such as railways (Jafarian and Rezvani, 2012; Zhang et al., 2020), nuclear (Jung et al., 2020; Purba et al., 2011), maritime (Akyuz et al., 2020; Kuzu et al., 2019), and Oil & Gas (Badida et al., 2019; Ikwan et al., 2021; Liaw et al., 2023; Yuhua and Datao, 2005).

Although it has several advantages and benefits, any FTA conceals major drawbacks (Yazdi et al., 2023). For instance, a FTA requires the knowledge of failure and repair data, which could be scarce. Thus, researchers have incorporated FTA with expert elicitation and Fuzzy Set Theory (FST) to overcome such limitations (Lavasani et al., 2015; Mahmood et al., 2013; Mentes and Helvacioglu, 2011). Additionally, it is a usually a static technique, which takes into account just a single kind of operation throughout the lifetime of a given system (Kabir, 2017). For this reason, various approaches such as Dynamic Fault Trees (DFT) (Dugan et al., 1997) and State/Event Fault Trees (Kaiser et al., 2007) have been developed. Furthermore, FTA assumes that the component failure events composing the FT are independent and the occurrence of one event thus not influence the likelihood of the others. This is a significant limitation since there could be strong dependencies among the components. For instance, there could be devices characterized by common cause failures, warm standby, or there could be limited resources for maintenance activities. FTs can model hot standby, characterised by a probability of failure of the standby component that does not change between the active and standby state. There is no dependency between the active and standby component. On the other hand, FTs are not able to model a warm or cold standby since there is a dependency between the active and standby components. The failure of the active component causes the standby to move from the dormant to the active

* Corresponding author.
E-mail address: filippo.decarlo@unifi.it (F. De Carlo).

https://doi.org/10.1016/j.jlp.2025.105545
Received 10 June 2024; Received in revised form 8 October 2024; Accepted 3 January 2025
Available online 8 January 2025

state, changing its probability of failure. Finally, FTs are unable to include complex maintenance strategies (Andrews and Tolo, 2023), such as opportunistic maintenance, condition-based maintenance, or predictive maintenance. Nevertheless, introducing the former features have progressively become more common as the complexity of the systems has increased, along with impressive advancements in technologies (e.g., sensors). To cope with the limitations of traditional FTA scholars have coupled the FT with Petri Nets (PNs) (Wu et al., 2011; Zhang et al., 2009) and Markov Models (Yevkin, 2016) to model higher complexity systems. Their results can be integrated into the results arising from the FT. This allows for a more realistic representation of the failure natures and behaviours.

Very recently, Andrews and Tolo (2023) have introduced the algorithm named Dynamic and Dependent Tree Theory (D^2T^2) to overcome typical limitations of the FT such as independent events, and the inability to model complex maintenance strategies. The authors have successfully applied the method to the cooling system of a pressure vessel, proving the advantages of the framework. Indeed, they were able to model opportunistic maintenance, non-constant failure rates, and warm standby. The results of the approach are promising; however, it could be interesting to investigate its effectiveness on other case studies. Indeed, the FT is a general technique, which is adopted in several different fields. Even though D^2T^2 has already been applied to a case study, it is required to test it on multiple case studies to determine its generalizability capabilities. Safety barriers are an interesting application since they have peculiarities, which make them different compared to other critical systems.

In its original version, the D^2T^2 has not been developed for a safety barrier, thus, it requires some amendments to be able to consider typical aspects of safety barriers. The objective of this paper is to extend the application of the D^2T^2 framework to safety barriers. As a matter of fact, the failure of a safety barrier could either be on demand or while running (after the demand, the system should operate for a given amount of time). During the standby phase, the components are usually inspected to detect hidden failures. In the operating phase, there is usually no possibility to inspect or maintain components. Finally, there are some components that are required to work only at the activation, while others should work for a prolonged period of time. It follows that the standby phase and the operational phase should be studied separately through an availability analysis and a reliability analysis respectively (Meshkat et al., 2000). The original framework marginally distinguishes between devices that fail on demand and devices that are required to operate until the system function is required. PNs and Markov models are only built for the operational phase. However, safety barriers need two separate analyses. For instance, a Markov model or a PN may be required to estimate the availability of a component, which is only required to work on demand. Thus, the Markov model and PN are not required for the reliability analysis. Another example is a component that may not be characterised by complexities or dependencies during the standby phase, leading to a traditional availability analysis (i.e., no Markov model or Petri Net). In turn, it may have a dependency during the operational phase, and it may be required to work for a prolonged time. This leads to the development of a PN or Markov model for the reliability analysis. These updates are required to apply the framework to a safety barrier, and this paper tries to address them. In this paper, an offshore fire deluge system is considered as case study. The offshore fire deluge system has been chosen for two main reasons. First, the offshore fire deluge system is a safety barrier and, as such, it spends most of its time in a standby condition. Additionally, the Oil & Gas industry is one of the most important with regards to reliability and risk analyses, and FTs are strongly employed. Moreover, FTA has already been applied to a fire deluge system (Andrews and Dugan, 1999; Bougofa et al., 2022; Guetarni et al., 2019; Landucci et al., 2015). Accordingly, proving the effectiveness of the D^2T^2 in a very common field of the FT is important. This application is helpful to further validate the D^2T^2 framework for systems that feature the sort of dependencies and complexities experienced in the offshore oil and gas production industry.

As a reminder, the remaining contents of the paper are as follows. In Section 2 the core material and methods are presented, while in Section 3 the D^2T^2 algorithm and its extension for a safety barrier are described. Section 4 is dedicated to the application of the extended methodology to an offshore fire deluge system. Finally, in Section 5 the discussions are illustrated, while Section 6 contains the conclusions, limitations, and potential future developments.

2. Constituent modelling methodologies

This section briefly presents the main concepts behind the core tools considered for this study.

2.1. Fault tree

FT is a logic tree structure used to express the causality of a specific system failure mode introduced in 1960 by Watson, 1961. Indeed, FT can incorporate both the logic behind a top event generation and a mathematical model to estimate the probability or frequency of the top event occurrence. Traditional FTA is characterized by two subsequent stages. The first stage consists of identifying the Minimal Cut Sets (MCSs) required to produce the top event. A MCS is defined as the necessary and sufficient events able to cause the top event. The second stage is conducted to estimate the frequency or probability of the top event. Any FT defines the relationship between component failure modes through AND and OR gates. An AND gate describes events that are all required to cause the upper event. An OR gate is used for a set of events where the occurrence of at least one is sufficient to cause the upper event.

To estimate the probability of the top event, the MCSs are considered along with the component failure probabilities. Specifically, a qualitative analysis is conducted first. The top event (TE) failure is expressed in terms of the MCSs as shown in Equation (1).

$$TE = C_1 + C_2 + \ldots + C_n \tag{1}$$

where $C_i, i = 1, \ldots, n$ represents the i-th MCS. The MCS are then expressed as conjunctions of basic events as denoted by Equation 2

$$C_i = X_{i1}.X_{i2}\ldots.X_{im} \tag{2}$$

where $X_{ij}, j = 1\ldots m$ are the basic events that compose the i-th MCS.

After the qualitative analysis, the quantitative analysis is carried out to estimate the probability of the top event. The main assumption of the FT is that the basic events are independent, thus, the probability of the top event can be obtained through Equation (3).

$$P_{TE} = \sum_{i=1}^{n} P(C_i) - \sum_{i=2}^{n}\sum_{j=1}^{i-1} P(C_i \cap C_j) + \sum_{i=3}^{n}\sum_{j=2}^{i-1}\sum_{k=1}^{j-1} P(C_i \cap C_j \cap C_k) - \ldots + (-1)^{n+1} P(C_i \cap C_2 \ldots \cap C_n) \tag{3}$$

For real practical applications, there are usually many MCSs characterizing a FT, thus, it could be unfeasible to evaluate Equation (3). Thus, an upper bound approximation of the probability of TE is obtained through the Minimal Cut Set Upper Bound shown in Equation (4).

$$P_{TE} \leq 1 - \prod_{i=1}^{n} (1 - P(C_i)) \tag{4}$$

2.2. Modularization

For real practical applications, FTs can be large and complex. Thus, they could be difficult to study and analyze. However, it is possible to conduct a modularization process, which allows to redefine the original FT, building a set of independent modules. Then, each module could be solved separately, and all the single solutions integrated. Before going

into details regarding a typical modularization process, it is required to introduce two definitions: initiating event and enabling event. An initiating event causes a demand on the protection systems to respond, while an enabling event is an inactive control or protection system which allows an initiating event to produce the top event.

D^2T^2employs a modularization approach performed in two phases. The first is evolved from a method called FAUNET (Platz and Olsen, 1976) composed of three subsequent steps named, contraction, extraction, and factorization. The second phase then uses a modification of the linear time algorithm proposed by Dutuit and Rauzi (Dutuit and Rauzy, 1996).

During the contraction step, subsequent gates of the same type are contracted into a single one. The second stage of the modularization methods consists in defining factors as one of the following categories.

- All events in the factor are independent initiating events
- All events in the factor are independent enabling events
- The factor contains all the events in a dependency group (i.e., common cause failures)

The probability of a factor can then be extracted through Equation (5) and Equation (6). Equation (5) refers to factors composed of independent events under an OR gate: $FAC_i = X_1 + X_2 + \ldots + X_n$. Equation (6) refers to factors composed of independent events under an AND gate: $FAC_i = X_1.X_2.\ldots.X_n$.

$$P_{FAC_i} = 1 - \prod_{j=1}^{n}\left(1 - P_{X_j}\right) \tag{5}$$

$$P_{FAC_i} = \prod_{j=1}^{n}\left(P_{X_j}\right) \tag{6}$$

The final stage of the modularization process is called extraction. It consists in redefining the tree by extracting a repeating event. At the end of the former modularization, the fault tree will be reduced. The obtained structure will be composed by and a core fault tree (eventually composed of factors) and a set of factors. The linear-time algorithm of Dutuit and Rauzi is applied to identify independent sub-trees, which is performed by assigning the same dependency group to the basic events of the sub-tree.

2.3. Binary Decision Diagram

A Binary Decision Diagram (BDD) can be obtained directly from a FT, and it has advantages when quantifying the top event probability. It is possible to transform this diagram into one which encodes the MCS (Akers, 1978). To build a BDD, it is required to consider a convenient ordering of the basic events composing the FT. The efficiency of the BDD analysis is dependent upon the variable ordering used.

The BDD is a directed acyclic graph, whose leaves are labeled with 0 and 1 (Ruijters and Stoelinga, 2015). The paths that end with 1 represent causes of the top event, while the paths that end with 0 are associated with the absence of the top event. Considering all the paths that end with 1, it is possible to obtain the top event probability as the sum of the probability associated with each path in case of mutually disjoint paths (see Equation (7)).

$$P_{TE} = \sum_{i=1}^{n} P(Path_i) \tag{7}$$

2.4. Markov Models

A Markov model allows to model systems or devices characterized by constant failure and repair rates. In other words, the system's failure behavior is memoryless, and it can be described through a Homogenous Poisson Process (HPP). A Markov model is composed of nodes and edges. The first represent states of the system, while the latter identify the transitions. The system evolves from node to node with eth state residence times being represented by the exponential distribution. From a mathematical perspective, the state equation is obtained as shown in Equation (8).

$$\dot{Q}(t) = Q(t)[A] \tag{8}$$

where Q and A are the vector of state probabilities and the state transition rate matrix respectively. The transition rate matrix contains the rates of switching between states (Liu, 2020).

It is worth mentioning that PNs and Markov models share similarities. However, PNs are more general and allow to represent a higher level of complexities. On the other hand, Markov models are less computationally expensive.

2.5. Petri Nets

A PN is a bi-partite graphical model composed of places, transitions, and arcs (Zhou and Reniers, 2020). The places and the transitions are usually represented by circles and rectangles respectively. Each place represents a different state of the modelled system (or device), while each transition represents an event (e.g., a failure), which leads to a change in the state of the system. The state of the system is denoted by the locations of a set of tokens in different places. The former distribution is called a 'marking'. The tokens are identified by black dots on the PN diagram. Finally, a set of arcs links places and transitions. Specifically, there are two different kinds of arcs: input arcs and output arcs. The first connects a place to a transition, while the latter connects a transition to a place. The arcs also have an associated with a multiplicity, whose standard value is one.

A Stochastic Petri Net (SPN) is a practical evolution of PN, a method that allows to model discrete event systems, allowing to identify behaviors and performance (Wang et al., 2024). They are often used for reliability problems. A SPN takes into account the concept of time compared to simple PN (Elusakin and Shafiee, 2020). Considering a SPN, it is possible to estimate relevant parameters through Monte Carlo Simulation. For instance, it could be possible to estimate the availability of a system or a component. The marking of the PN will change over time due to transitions firing. Accordingly, the system would evolve dynamically over time according to a set of rules. A transition is enabled when each input place linked to the transition has at least the number of tokens equal to the multiplicity of the corresponding arc. After a transition is enabled, it will fire after a time interval randomly drawn from the associated distribution. When the transition is fired, the multiplicity of tokens is removed from the input places and a multiplicity of tokens is sent to the output places.

3. Dynamic and dependent tree Theory methodology

The D^2T^2 has been recently developed by Andrews and Tolo (Andrews and Tolo (2023). D^2T^2 has been proposed to cope with typical limitations characterising any FTA. As reported by the authors (Andrews and Tolo, 2023), D^2T^2 offers a solution for:

- Enabling the representation of non-constant failure and repair rate, which could be modelled through any probability distribution
- Including all possible dependencies and complexities among different events. For instance, the dependencies could be related to failure behaviours (e.g., common cause failures)
- Allowing the inclusion of complex maintenance strategies typical of modern systems. Examples are opportunistic, condition-based, and predictive maintenance

Moreover, D^2T^2 maintains the FT structure to represent the logic behind the generation of an undesired top event extending the abilities of the FTA thanks to the integration of BDD, PNs, and Markov models. Specifically, when the considered system is characterized by non-

constant failure or repair rates, a PN could be considered to model the former scenario. For given complexities or dependencies either a PN or a Markov model could be developed. In this context, it is worth mentioning that the smallest PN or Markov model should be considered for computational efficiency purposes. If possible, a Markov model should be preferred over a PN since it is less computationally expensive. Since the adopted Markov models and PNs are detached from the FT, it is required to integrate their results into the FT. This is possible thanks to the modularization and the subsequent construction of the BDD. The approach is shown in Fig. 1, where the light blue ovals represent the input files, the grey ovals identify intermediate files, and the orange rectangles represent the steps required to in the approach. The upper part represents the original framework, while the lower part identifies the modified framework to extend the analysis to safety barriers.

As shown in Fig. 1, there are three different input files: i) the fault tree structure file, ii) the component repair and failure rate information file, and iii) the dependency file. The third file reports the system complexity and dependencies. To implement the algorithm, the following seven steps are pivotal.

i. Identify the initiating and enabling events.
ii. Define and create the dependency groups, i.e., all the events subjected to the same dependency should be grouped together. Compared to the original framework, it is also required to distinguish between dependencies of the standby phase and operating phase.
iii. Quantify the failure probabilities of the independent components through the traditional methods. Compared to the original framework, components that fail on demand and components that are needed for a prolonged period of time are distinguished. This also serves to identify PNs and Markov models required for the availability and reliability analyses.
iv. Conduct the modularization
v. Develop PNs and Markov models for the considered dependencies and solve these dependency modules. Compared to the original framework, this step is conducted separately for the standby and operational phases. The Markov models and PNs of the operational phase are fed with the results of the availability analysis.
vi. Build the BDDs corresponding to the FT modules.
vii. Integrate the results arising from the PNs and Markov models into the BDD. Predict the top event probability.

Based on these steps, the D^2T^2 algorithm can incorporate complexities and dependencies, overcoming some typical limitations of the FT. Accordingly, the D^2T^2 approach could allow to obtain a more realistic and appropriate representation of the studied system. The original framework is sufficient in case an operational system is considered. However, some amendments are required to model safety barriers. Specifically, it is required to distinguish between the dependencies and complexities characterizing the standby and operating phases respectively. Indeed, there could be some differences between the two phases. Subsequently, the PNs and Markov models are developed for the standby phase. These PNs and Markov models are fundamental to predict the probability of a component of being in a given state when the system demand occurs. The (initial) state of a component at this point in time influences the ability of the system to operate. Next, the PNs and Markov models of the operating phase are built. This phase is performed only for the components that are required to operate for a prolonged period. The initial states' probabilities are set according to the availability analysis. Finally, the calculation is run also for the PNs and Markov models of the operating phase, and their results are integrated with the BDD.

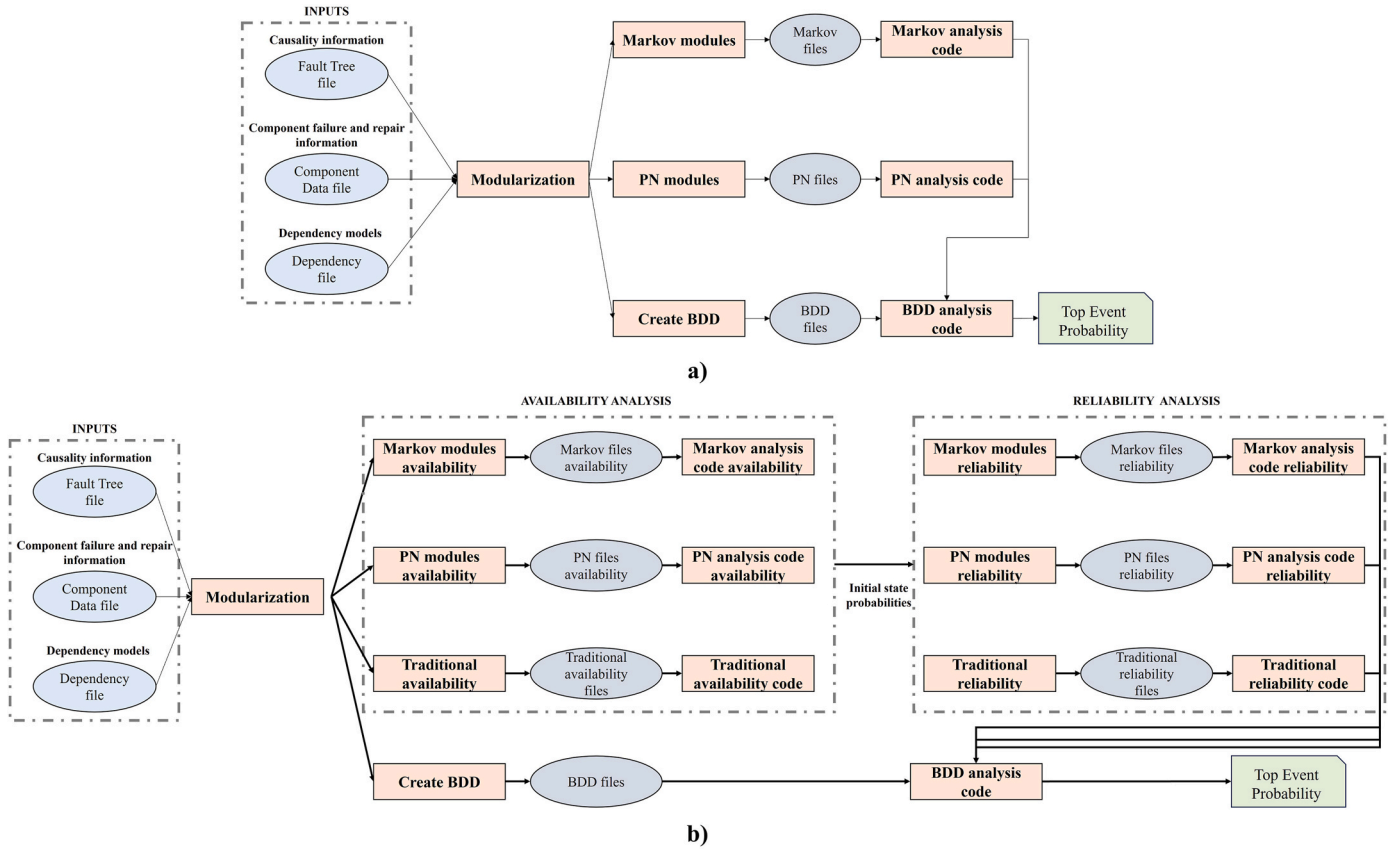


Fig. 1. Original framework (a) and updated framework for safety barriers (b).

4. Application of the methodology to an offshore fire deluge system

4.1. Case study: offshore fire deluge system

An offshore fire deluge system is a safety barrier located in offshore platform. It is activated in case of a fire occurring in one of the offshore platform's modules. A schematic representation of an offshore fire deluge system is shown in Fig. 2.

The water is distributed around the platform through a ring main. The water is pressurized through a jockey pump. Under the event of a fire in one of the offshore platform's modules (e.g., the separation module), the system will activate. Two sensors are devoted to detecting the presence of the fire, a Heat Sensor (HS) and a Smoke Sensor (SS). When at least one of the two sensors detect the fire, a signal is sent to the Display Panel (DP), which reveals the presence of fire to the Operator (OP). The operator presses a Button (BT), and the system is activated.

The activation button opens the Valve (V1). Water then flows from the main ring to the dry distribution pipes, reaching the sprinkler nozzles (NOZ). Accordingly, the water is fed to the area where the fire occurred. Since the water is flowing out of the ring main, a pressure reduction would occur. Three pressure sensors (S1, S2, and S3), are responsible for monitoring the pressure inside the ring main. When at least two of the three sensors detect a pressure drop, the signals sent to the Computer (COMP) are processed, which activates an electric pump (P1). In case either the electric pump, the electric motor, or the electric supply fails, a backup diesel pump (P2) is activated instead. This task is performed by a pump changeover system composed of a sensor in charge of detecting the failure (SEN1) and a pump controller (CONT). The diesel pump is served by a diesel motor and a diesel supply. The pumps take water from the sea through two water supplies (T1 and T2), which provide the required water to the offshore fire deluge system.

There are several complexities and dependencies in the offshore fire deluge system to be considered.

- The water supplies degrade over time even if the system is not required. They are inspected periodically once every year. Both have three different states: working, degraded, and failed. In case a degraded or failed condition is detected, opportunistic maintenance is conducted.
- The time to failure of the motors follow an exponential distribution during the stand-by period, while it follows a Weibull distribution during the operating period. Indeed, it is assumed that motors are subjected to random failures when non-operating, while they are characterized by wear during the operating phase. Previous works have also adopted an exponential distribution for the non-operating phase and a Weibull distribution for the operating phase (Pan, 1998).
- Pressure sensors are subjected to common cause failures.
- The diesel pump system is in cold standby with the electric pump system. Therefore, it is guaranteed to work in the event that one of the electric devices (i.e., pump, motor, and supply) has failed.

The considered system is a safety barrier and would normally be in a standby state, during which all the components are assumed to be inspected every three months (approximately 2190 h). In addition, it is assumed that the system would need to work for a maximum of 24 h in the presence of a fire. During this period, it is not possible to conduct maintenance activities. It is therefore required to define the PNs and Markov models for the dependencies characterizing the standby period and the dependencies of the 24-hour working period. In this context, among the complexities and dependencies listed above, only the pump system is required to operate for 24 h. The other complexities and dependencies are solely related to the standby phase. Indeed, the related devices are asked to work only at the activation. The top event for the FT is: "System fails to deliver water to the sprinklers in case of fire".

4.2. Analysis of offshore fire deluge system through the D^2T^2 algorithm

The FT and sub-tress for the top event is shown in Figs. 3–6. The FT is related to the operating condition since the reliability analysis should be conducted for the operating phase and the basic events are listed in Table 1.

Following the procedure described in the previous section, the initiating and enabling events are identified (step i). Since the offshore

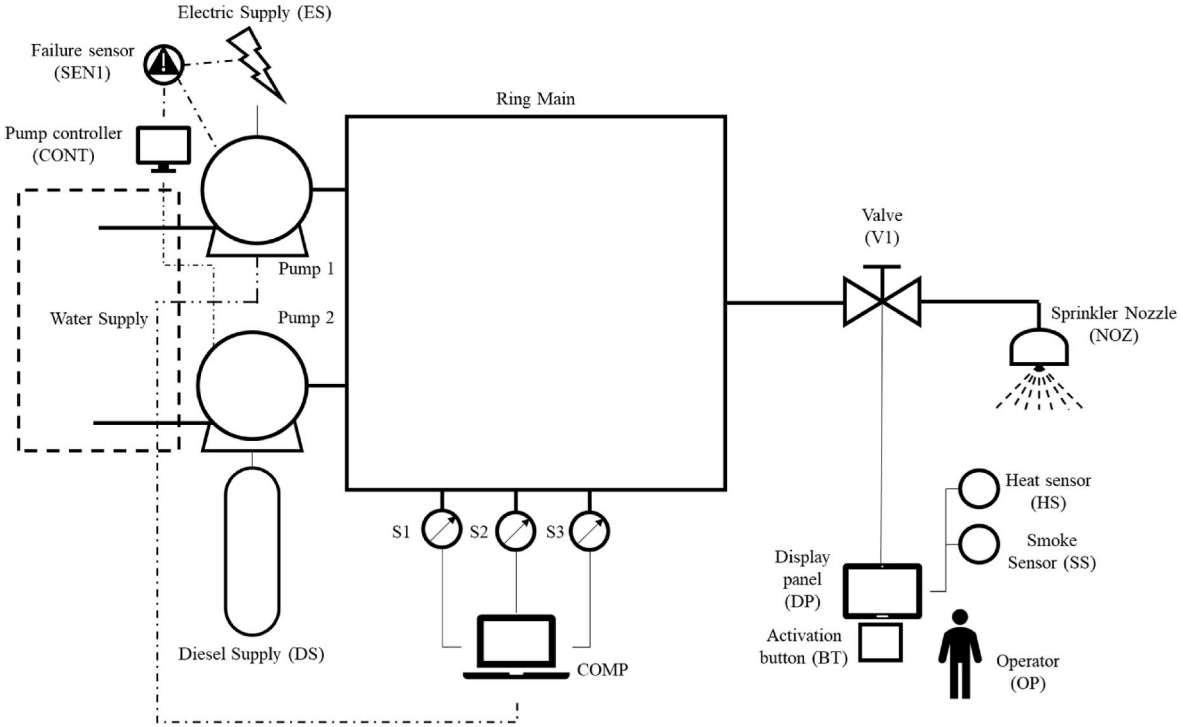


Fig. 2. Schematic representation of an offshore fire deluge system.

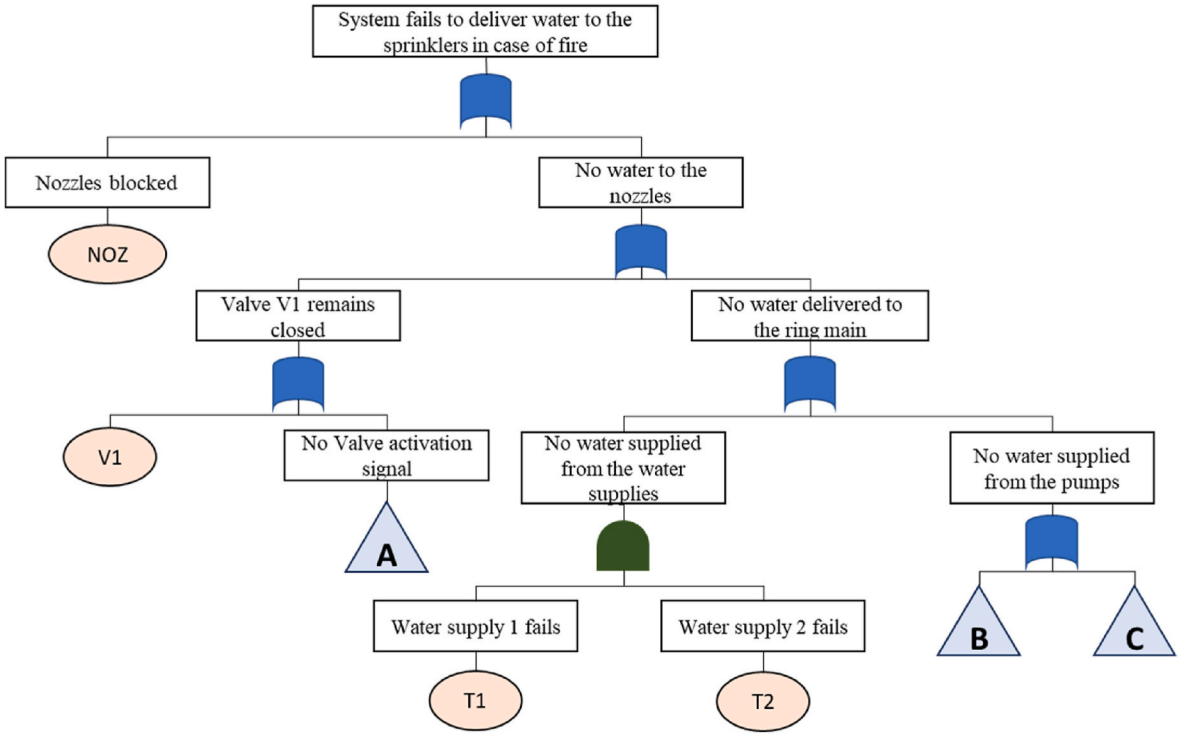


Fig. 3. Developed FT for the considered top event.

fire deluge system is a safety barrier, all the events are considered as enablers.

Then, step ii is conducted to define the complexity and dependency groups characterizing the developed FT. Compared to the original D^2T^2 algorithm, it is required to define the complexity and dependency for the standby and operational phase. The former represents the first amendment required to apply the approach to a safety barrier. Considering the standby phase, the first group is composed of the water supplies, which have three states during the standby period: as good as new (NEW), degraded (DEG), and faulty (FLT). These complexity groups are identified through Equations (9) and (10).

$$C1 = \{T1_{NEW}, T1_{DEG}, T1_{FLT}\} \tag{9}$$

$$C2 = \{T2_{NEW}, T2_{DEG}, T2_{FLT}\} \tag{10}$$

However, the water supplies are not independent during the standby phase since they are subjected to opportunistic maintenance. Thus, there is an additional dependency group as shown in Equation (11).

$$D1 = \{C1, C2\} \tag{11}$$

The other dependency group of the standby phase is related to the pressure sensors, which are subjected to common cause failures. Thus, they are included in the dependency group $D2$ as shown in Equation (12).

$$D2 = \{S1, S2, S3\} \tag{12}$$

Considering the operating phase, there are two complexity groups related to the motors since their failure behaviour is characterized by a Weibull distribution, characterised by a shape (β) and a scale (η) parameter. These complexity groups are shown in Equations (13) and (14) for the electric motor and diesel motor respectively.

$$C3 = \{EM\} \tag{13}$$

$$C4 = \{DM\} \tag{14}$$

It is worth noting that their failure behaviors is not totally independent since they are part of a standby sub-system (i.e., the pump system). Thus, they could not be modelled as standalone and a larger dependency group ($D3$) is defined. This dependency group includes all the devices which belong to the overall pump system (both electric and diesel). As a reference, see Equation (15).

$$D3 = \{P1, EM, ES1, P2, DM, DS\} \tag{15}$$

After the identification of the dependency groups, the traditional probabilities of failure are estimated (step iii). This step is conducted considering a periodic inspection for every component every three months (2190 h), both the inspection and maintenance are considered as perfect. The average probability of failure is given by Equation (16) (Andrews and Tolo, 2023).

$$P_{AV} = 1 - \frac{(1 - e^{-\lambda\theta})}{\lambda\theta} \tag{16}$$

where λ is the failure rate, while θ is the inspection interval. Equation (16) is used to conduct the availability analysis during the standby period. This equation provides the probability of a device being in a failed state when the deluge system is required and is adopted for each component that does not belong to a dependency or complexity group. It is also used for the components of dependency group $D3$ to derive the initial state probability. The fault tree basic events, along with the related dependency groups, are shown in Table 1, where the kind of failure is also shown. Specifically, two different kinds of failure are considered. The first kind is named “on demand”, which is associated with components whose failure is significant only when the fire deluge system is activated. However, after the initial activation, the reliability performance of these components is no longer relevant. In other words, they have to work only at the activation. On the other hand, the second kind of failure regarded as “On demand and while running” is assigned to components that are required to funcion both at the activation and throughout all the operating period. Therefore, they can either fail on demand or when the fire deluge system is running. Table 2 lists the failure rates and average probabilities of failure. The former failure characteristics are either based on literature or expert judgments. The

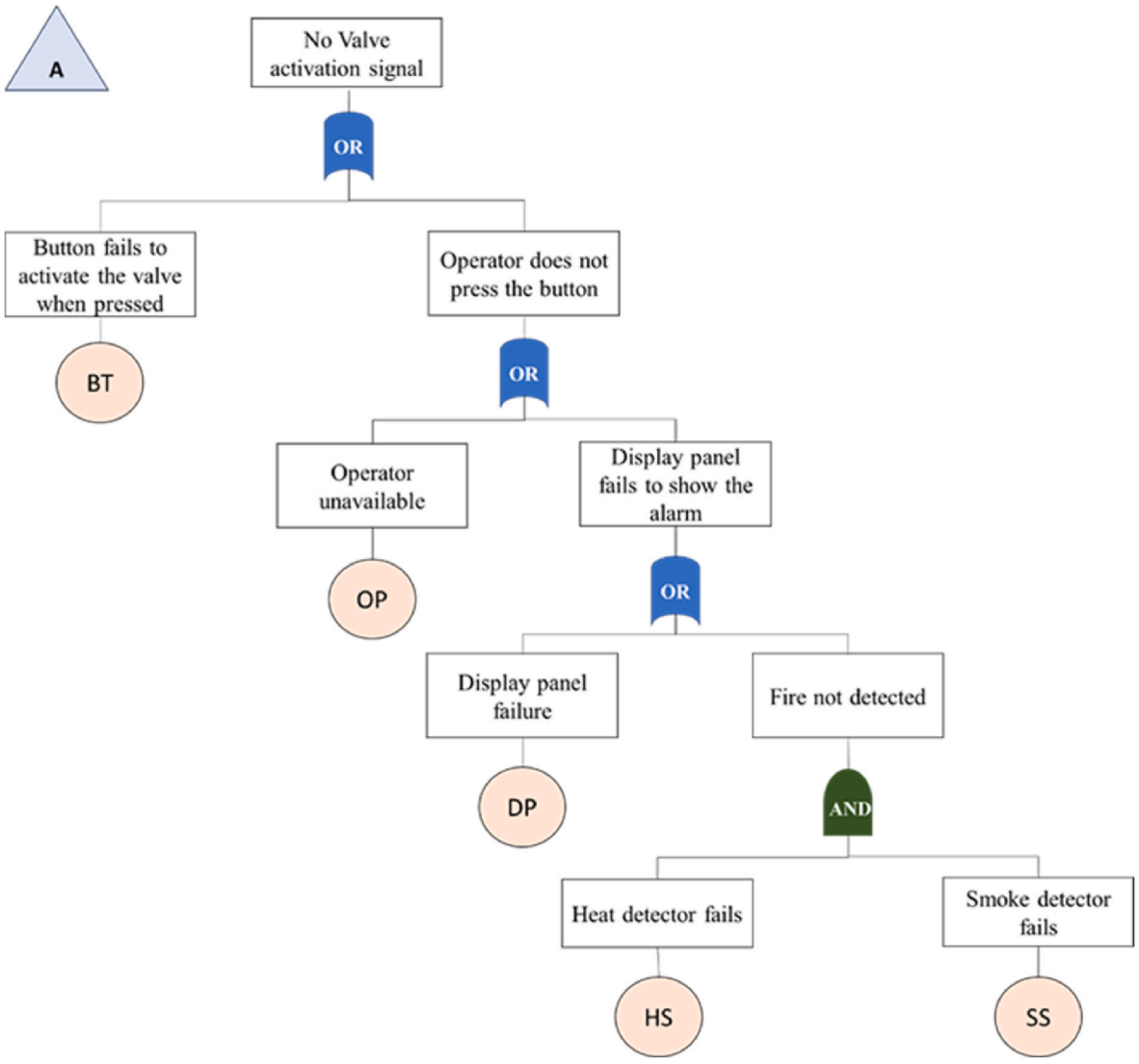


Fig. 4. Intermediate event "A" of the FT displayed in Fig. 3.

Weibull failure distribution of motors (Andrews and Tolo, 2023) and the failure rate of the nozzle (Bougofa et al., 2022; Guetarni et al., 2019) are directly taken from literature. The failure rates of pumps, pressure sensors, heat sensor, and smoke sensor are elaborated from available references (Andrews and Tolo, 2023; Bougofa et al., 2022; Guetarni et al., 2019). This choice is made since the identified values can vary from reference to reference. The remaining failure rates are determined through expert judgements during focus groups. This aspect does not reduce the quality of this study, which aim to present the improved version of the D^2T^2 and its advantages rather than extracting exact real-world data and implications. Companies will be able to do that by inserting their available data. This choice can also be found in previous works that considered numerical examples (Do et al., 2015; Hong et al., 2014; Leoni et al., 2022).

After the estimation of the traditional probabilities of failure, the modularization of the FT is carried out (step iv). The modularization process includes a factorization step. During the former step, the following factors are created:

$$Cf_1 = NOZ + V1 + BT + OP + DP + COMP + ES2 \ (independent\ enablers)$$

$$Cf_2 = HS.SS \ (independent\ enablers)$$

$$Cf_3 = T1.\ T2 \ (dependency\ group - -enablers)$$

$$Cf_4 = S1.S2 + S2.S3 + S3.S1 \ \ (dependency\ group - -enablers)$$

$$Cf_5 = SEN1 + CONT \ (Independent\ enablers)$$

Since Cf_1, Cf_2, Cf_3, Cf_4 are independent from all other events of the FT (even though two of them represent a dependency group), they could be grouped together into the following factor. This is done during the second factorization step. It is worth noting that between the first and second factorization, no contraction or extraction is possible.

$$Cf_6 = Cf_1 + Cf_2 + Cf_3 + Cf_4 \ (Independent\ enablers)$$

Finally, following the liner-time algorithm of Dutuit and Rauzy, it is possible to model the top gate considering two modules: Cf_6 and G1. G1 identifies the remaining part of the FT, composed of mainly dependent events that could not be further reduced. The modules can be analyzed separately. The results of the modularization process are shown in Fig. 7.

Following the modularization, the PNs and Markov models associated with the identified complexities and dependencies are developed (step v). In this context, the water supplies and the pump system are modelled through PN. The pressure sensors are modelled through a Markov model. As previously mentioned, it is required to develop PNs

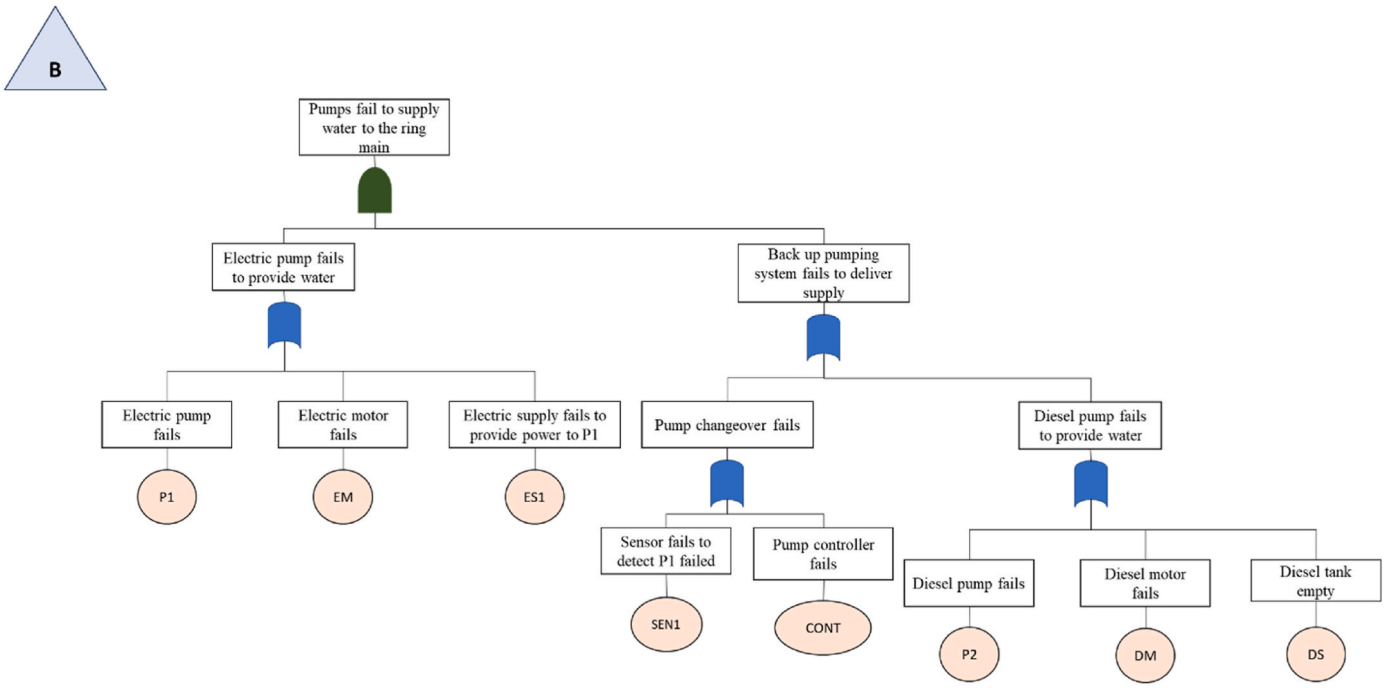


Fig. 5. Intermediate event "B" of the FT displayed in Fig. 3.

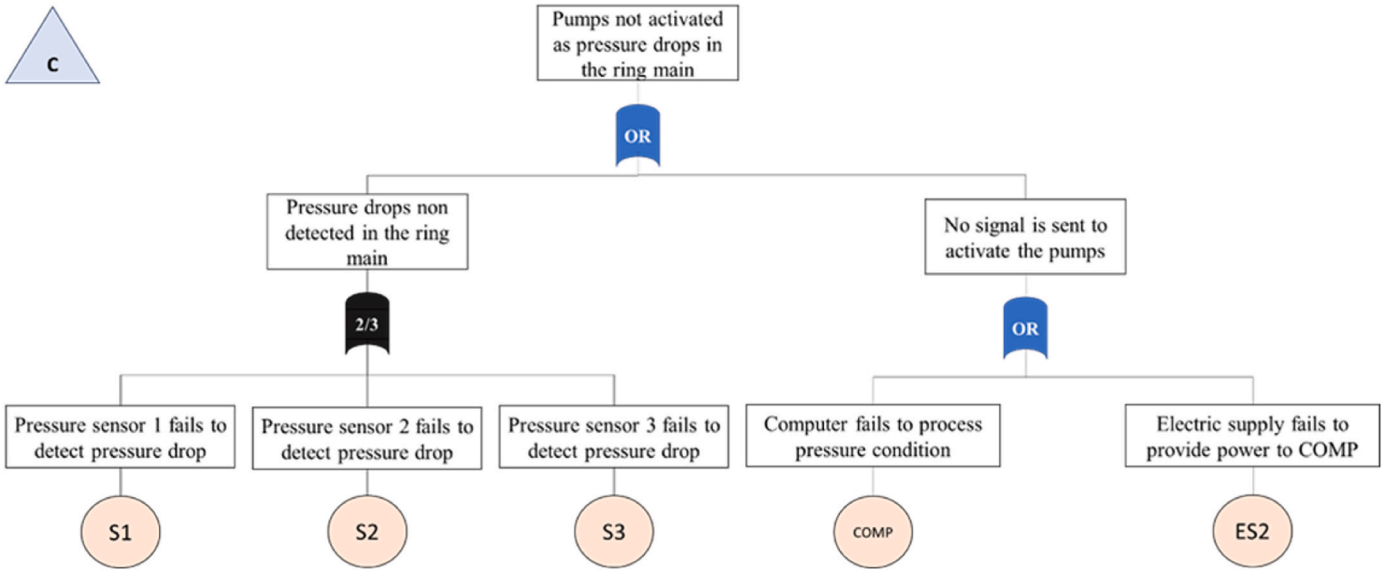


Fig. 6. Intermediate event "C" of the FT displayed in Fig. 3.

and Markov models during the standby phase and during the operating phase separately.

Considering first the complexity groups, the PN for the water supply dependency group (D1) is shown in Fig. 8. The green transitions represent the inspection (i.e., they are fired once a year if habilitated), while the red transitions denote the shift towards a worse condition (i.e., from new to degraded or from degraded to failed). Considering the green transitions, θ denotes the inspection interval, while λ_1 and λ_2 represent the failure rate of the water supplies from good to degraded and from degraded to failed reported in Table 2. The black transitions identify instantaneous repair since the repair time is assumed negligible compared to the time the water supplies spend in the other states. Considering the nodes, "T1_Rep_Deg" and "T1_Rep_Failed" represent repair states of the first water supply after it is identified as degraded and failed respectively. Similarly, "T2_Rep_Deg" and "T2_Rep_Failed" denote the repair state of the second water supplies when its condition is evaluated as degraded and failed respectively. Finally, "T1&T2_Rep" means that both water supplies are being repaired since both are in a failed state. These nodes make the PN more comprehensive for potential future studies that focus on the repair actions (e.g., comparing different repair solutions or technologies).

The PN is related to a standby period, and it is simulated for a 30 year period, giving the results shown in Table 3. The PN models were developed through the Petri Net Sotware developed by TotalEnergies (https://grif.totalenergies.com/en/products/simulation-package/module-petri). The software allows to conduct the simulation through the Monte Carlo – Petri Nets approach. Specifically, when a transition is habilitated, a random time is extracted via Monte Carlo based on the

Table 1
Components, failure modes, labels, and dependency groups for both the standby and operating phase.

Component Name	Failure Mode	Label	I/E	Kind of failure	Dependency group
Electric Motor	Fails	EM	E	On demand and while running	D3
Diesel Motor	Fails	DM	E	On demand and while running	D3
Electric Pump	Fails	P1	E	On demand and while running	D3
Electric Power Supply to P1	Fails	ES1	E	On demand and while running	D3
Diesel Pump	Fail to start	P2	E	On demand and while running	D3
Diesel Supply to P2	Tank Empty	DS	E	On demand and while running	D3
Pump failure sensor	Fails to detect P1 failed	SEN1	E	On demand	
Pump controller	Fails	CONT	E	On demand	
Water supply 1	Failure of water supply	T1	E	On demand	D1
Water supply 2	Failure of water supply	T2	E	On demand	D1
Pressure Sensor 1	Fails High	S1	E	On demand	D2
Pressure Sensor 2	Fails High	S2	E	On demand	D2
Pressure Sensor 3	Fails High	S3	E	On demand	D2
Electric Power Supply to COMP	Fails	ES2	E	On demand	
Computer	Fails	COMP	E	On demand	
Display Panel	Display fails	DP	E	On demand	
Activation Button	Fails	BT	E	On demand	
Operator	Unavailable	OP	E	On demand	
Valve	Fails to Open	V1	E	On demand	
Heat Sensor	Fails to Register Fire	HS	E	On demand	
Smoke Sensor	Fails to Register Fire	SS	E	On demand	
Nozzle	Blocked	NOZ	E	On demand	

probability distribution associated with the transition. After the random time has passed, if no other event modifying the state of the system has occurred, the transition fires the token from the input node to the output node. This allows the system to evolve over time. Tracking the time that the tokens spend in each node, it is possible to extract the probabilities of the system of being in different states (i.e., different token distributions across the nodes). In the PN, a fictional variable is used to maintain an as good as new water supply in case the other is in a degraded or failed state. Specifically, the value of the fictional variable was set to 1 in case at least one water supply is in a degraded or faulty state. It is reset to zero when the as good as new condition is restored. In case a water supply is in an as good as new condition and the other is either degraded or faulty, the fictional variable is equal to 1. This condition triggers the maintenance also on the as good as new water supply.

Considering the dependency group related to the pressure sensor (D2), a Markov model is developed as shown in Fig. 9. The Markov model is composed of 4 nodes. The first node (3Sw) is characterized by all the pressure sensors working. The second (2Sw), the third (1Sw), and the fourth (0Sw) correspond to two sensors working, one sensor working, and no sensor working respectively. The Markov model is valid for the standby phase, considering a mean repair time equal to 5 h. The

Table 2
Failure rate and probability of failure considered for each device.

Label	Failure rate [events/hours]	Probability of failure on demand
P1	Standby: 0.000001 Work: 0.0001	0.00109
ES1	0.000005	0.00546
EM	Standby: 0.000001 Work: beta = 1.5; Eta = 12,000	0.00109
P2	Standby: 0.0000005 Work: 0.00005	0.000547
DS	0.000004	0.00437
DM	Standby: 0.0000005 Work: beta = 1.5; Eta = 12,000	0.000547
S1	0.000002 CCF = 0.000001	
S2	0.000002 CCF = 0.000001	
S3	0.000002 CCF = 0.000001	
ES2	0.000005	0.00546
COMP	0.000001	0.00109
DP	0.000005	0.00546
BT	0.000005	0.00546
OP		0.001
V1	0.0000075	0.00817
HS	0.000005	0.00546
SS	0.000008	0.00871
NOZ	0.000001	0.00109
T1	New to deg: 0.00001 Deg to fail: 0.0001	
T2	New to deg: 0.00001 Deg to fail: 0.0001	

results associated with the Markov model of the pressure sensors during the standby period are listed in Table 4. The CCF has been added to the model by inserting a link between each of the first three nodes and the last one. The link reports a failure transition equal to the common cause failure one.

These PN and Markov model are related to the standby phase. The results arising from the models are used to estimate the probability of failure on demand. It is assumed that both the water supplies and the sensors should only work at the activation of the system. However, there is an additional dependency group (D3) related to the operating phase. This group is modelled through a PN (see Fig. 10) considering the diesel pump system in cold standby with the electric pump system. The initial probability of failure considered for the PN are estimated through Equation (16) for each component. As mentioned for the PN of the water supplies, the red transitions identify the switch to a worse state, while the black transitions are instantaneous ones. The failure parameters of the red transitions are the ones listed in Table 2. Each electrical pump system component is in a standby state at the beginning. Through an instantaneous transition each component is either sent to a failed or new state. The probabilities of being in one of the two states are estimated through Equation (16) and they are shown in Table 2. When an electrical pump system's component fails, the electrical pump system is considered failed, and a demand is put on the diesel pump system. The diesel pump system is in a standby state at the beginning as shown by the corresponding token in Fig. 10. When the diesel pump system is activated, a demand is put on all its components. These are sent through instantaneous transitions to a failed or new state, following the approach adopted for the electric pump system's components. When one of the

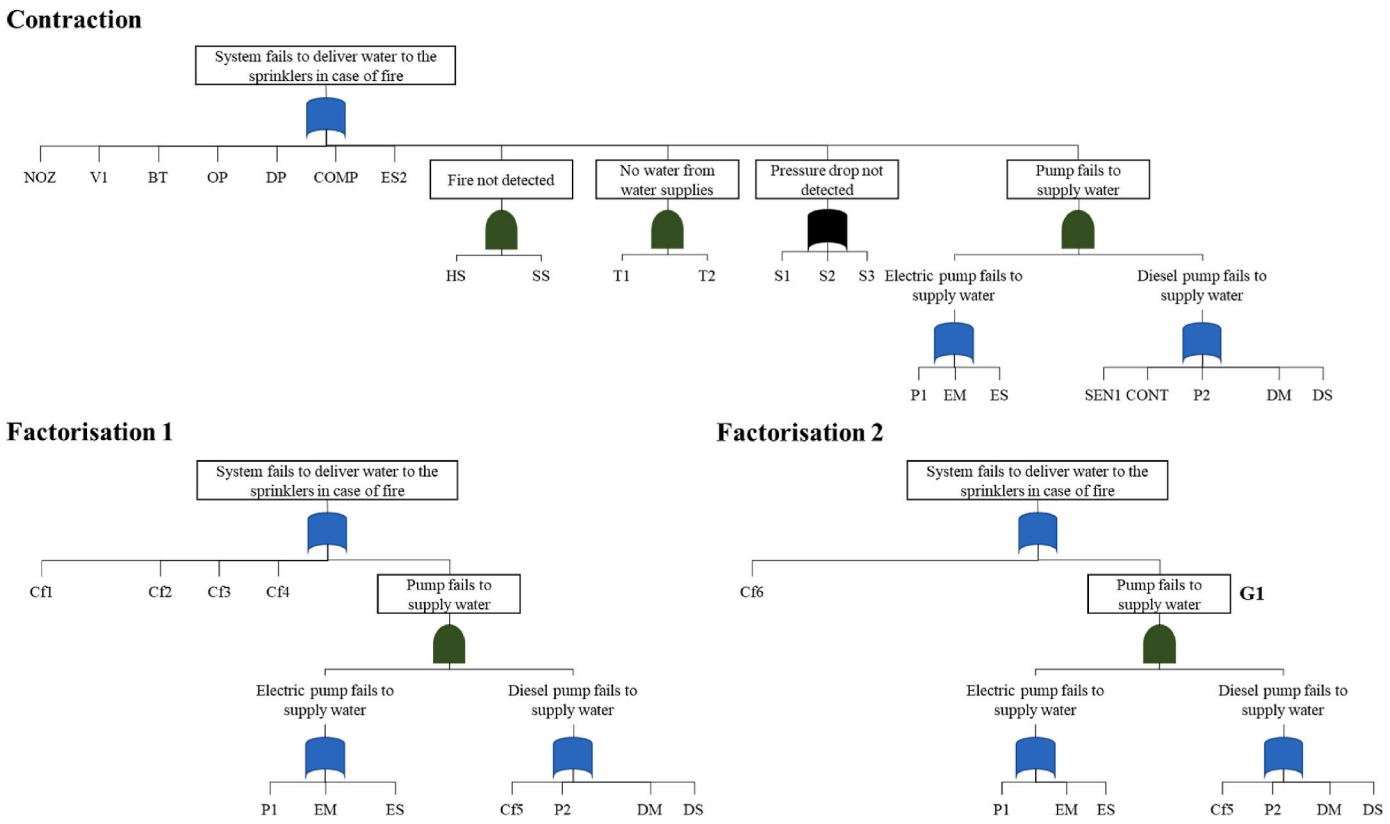


Fig. 7. Modularization of the considered FT.

diesel pump system's components fails, the whole pump system is considered as failed.

Considering the first dependency group of the operating phase (i.e., D3), a PN is developed adopting GRIF software and the Monte Carlo approach previously described. The PN considers all the components of the pump system. The PN is simulated for 24 h and probabilities of the critical states are tracked down as shown in Equations (17)–(28).

$$P(P1) = 0.00229843 \tag{17}$$

$$P\left(EM_f|P1_w\right) = 0.001145938 \tag{18}$$

$$P\left(ES_f|P1_w, EM_w\right) = 0.005521945 \tag{19}$$

$$P\left(P2_f|P1_f\right) = 0.00000268 \tag{20}$$

$$P\left(DM_f|P1_f, P2_w\right) = 0.00000047 \tag{21}$$

$$P\left(DS_f|P1_f, P2_w, DM_w\right) = 0.00000989 \tag{22}$$

$$P\left(P2_f|P1_w, EM_f\right) = 0.00000151 \tag{23}$$

$$P\left(DM_f|P1_w, EM_f, P2_w\right) = 0.0 \tag{24}$$

$$P\left(DS_f|P1_w, EM_f, P2_w, DM_w\right) = 0.00000566 \tag{25}$$

$$P\left(P2_f|P1_w, EM_w, ES_f\right) = 0.00000490 \tag{26}$$

$$P\left(DM_f|P1_w, EM_w, ES_f, P2_w\right) = 0.000002 \tag{27}$$

$$P\left(DS_f|P1_w, EM_w, ES_f, P2_w, DM_w\right) = 0.00002982 \tag{28}$$

The sixth step (step vi) consists in building the BDD. The BDD is developed for the sub-tree containing the dependent events (i.e., G1). Considering the following order of the variables involved $P1 < EM < ES1 < Cf_5 < P2 < DM < DS$, the obtained BDD is shown in Fig. 11.

The probabilities of the required events are estimated through PNs and integrated with the developed BDD. There are 12 possible paths, whose probability are expressed in Equations (29)–(40). Using the liner-time algorithm of Dutuit and Rauzy, it is possible to model the top gate considering two modules: Cf_6 and G1. Summing all the mutually exclusive path probabilities, gives the probability of G1 is approximately 5.88E-05.

$$P(Path_1) = P(P1).P\left(Cf_5\right) = 1.50393E-05 \tag{29}$$

$$P(Path_2) = P(P1).\left(1 - P\left(Cf_5\right)\right).P\left(P2_f|P1_f\right) = 6.12908E-09 \tag{30}$$

$$P(Path_3) = P(P1).\left(1 - P\left(Cf_5\right)\right).\left(1 - P\left(P2_f|P1_f\right)\right).P\left(DM_f|P1_f, P2_w\right) = 1.07934E-09 \tag{31}$$

$$(Path_4) = P(P1).\left(1 - P\left(Cf_5\right)\right).\left(1 - P\left(P2_f|P1_f\right)\right).\left(1 - P\left(DM_f|P1_f, P2_w\right)\right).P\left(DS_f|P1_f, P2_w, DM_w\right) = 2.25721E-08 \tag{32}$$

$$P(Path_5) = (1 - P(P1)).P(EM_f|P1_w).P(Cf_5) = 7.48099E - 06 \quad (33)$$

$$P(Path_6) = (1 - P(P1)).P(EM_f|P1_w).(1 - P(Cf_5)).P(P2_f|P1_w, EM_f) = 1.7099E - 09 \quad (34)$$

$$P(Path_7) = (1 - P(P1)).P(EM_f|P1_w).(1 - P(Cf_5)).(1 - P(P2_f|P1_w, EM_f)).P(DM_f|P1_w, EM_f, P2_w) = 0.0 \quad (35)$$

$$P(Path_8) = (1 - P(P1)).P(EM_f|P1_w).(1 - P(Cf_5)).(1 - P(P2_f|P1_w, EM_f)).(1 - P(DM_f|P1_w, EM_f, P2_w)).P(DS_f|P1_w, EM_f, P2_w, DM_w) = 6.42873E - 09 \quad (36)$$

$$P(Path_9) = (1 - P(P1)).(1 - P(EM_f|P1_w)).P(ES_f|P1_w, EM_w).P(Cf_5) = 3.60074E - 05 \quad (37)$$

$$P(Path_{10}) = (1 - P(P1)).(1 - P(EM_f|P1_w)).P(ES_f|P1_w, EM_w).(1 - P(Cf_5)).P(P2_f|P1_w, EM_w, ES_f) = 2.68068E - 08 \quad (38)$$

$$P(Path_{11}) = (1 - P(P1)).(1 - P(EM_f|P1_w)).P(ES_f|P1_w, EM_w).(1 - P(Cf_5)).(1 - P(P2_f|P1_w, EM_w, ES_f)).P(DM_f|P1_w, EM_w, ES_f, P2_w) = 1.09338E - 08 \quad (39)$$

$$P(Path_{12}) = (1 - P(P1)).(1 - P(EM_f|P1_w)).P(ES_f|P1_w, EM_w).(1 - P(Cf_5)).(1 - P(P2_f|P1_w, EM_w, ES_f)).(1 - P(DM_f|P1_w, EM_w, ES_f, P2_w)).P(DS_f|P1_w, EM_w, ES_f, P2_w, DM_w) = 1.63036E - 07 \quad (40)$$

Considering Cf_6, its probability is equal to 0.0276. Thus, combining Cf_6 and G1 into the factor Cf_7 gives a probability of the top event equal to 0.0277.

5. Discussion

D^2T^2 has been effectively applied to an offshore fire deluge system, which is a relevant safety barrier. As such, the offshore fire deluge system spends most of its time in a standby condition, becoming operational in the case of fire. The failure behaviours of the components and the maintenance policies vary between the standby and the working period. The standby phase affects both the probability of failure during the operations, and also their probability of failure on demand (Bucelli et al., 2018). This is the main amendment compared to the original framework (Andrews and Tolo, 2023). This amendment is required to extend the application of the approach to safety barriers or systems that spend most of their time in a standby condition. The D^2T^2 algorithm allowed the incorporation of complexities and dependencies in a FT, leading to the calculation of the top event probability. This task is accomplished thanks to the integration of the FT with Markov models and PNs, which have already been previously incorporated by some past works (Aslansefat et al., 2020; Ramezani et al., 2016; Talebberrouane et al., 2016; Zhu and Zhang, 2022). For the considered case study, the system has been modelled both during the standby period and during a 24-h working period. Two distinct PNs have been adopted to model the pump system and the water supply system respectively. A Markov model was sufficient to model the pressure sensor system characterized by common cause failures.

The water deluge system analysis could be included in an Event Tree (ET), which may also be integrated with models representing other subsystems such as the leak detection, isolation, blowdown and evacuation sub-systems to predict the expected consequences of the hazard (Tolo and Andrews, 2022). The undesired event is usually a loss of containment or the presence of fire, which puts a demand on a set of safety barriers. The accident sequence evolves through the interaction of barriers, whose proper function is fundamental for the failure or success outcome (Ramzali et al., 2015). It is essential to study both their probability of failure on demand and their probability of failure during the operating period.

Finally, the algorithm could be used to test different maintenance and inspection strategies for the system. The probability of failure of each component is strongly influenced by the selected maintenance and inspection policy and an analysis could compare multiple maintenance strategies, studying as a relevant driver the overall probability of the top event.

It is also worth noting that the framework could be used to include human errors, harsh weather conditions, or different forms of external events. Anyway, influencing factors cannot be considered by the present framework. These influencing factors will allow the probabilities of basic events to be changed but not guarantee the events will occur. Examples that will be better represented by this feature are the performance shaping factors that affect human probabilities, climate change issues that can affect many basic events, and environmental factors such as the situation of offshore platforms (the failure rates of components in the northern North Sea and the southern North Sea are different) or the environments of jet engines (heat, vibration, and humidity) that change the component failure rates. Moreover, the D^2T^2 framework requires the definition of a FT and a set of PNs and Markov models. This task is not a straightforward process and may represent a barrier for engineers that are not familiar with the techniques. In this context, few studies were conducted to automate FTA, and they did not provide a method that works well for control loops and electrical circuit structures.

6. Conclusions

This paper proposes the application of the D^2T^2 algorithm to an offshore fire deluge system, which is a safety barrier for an offshore platform. The D^2T^2 approach overcomes typical limitations of traditional FT methods through the integration of PNs, Markov models, and BDDs.

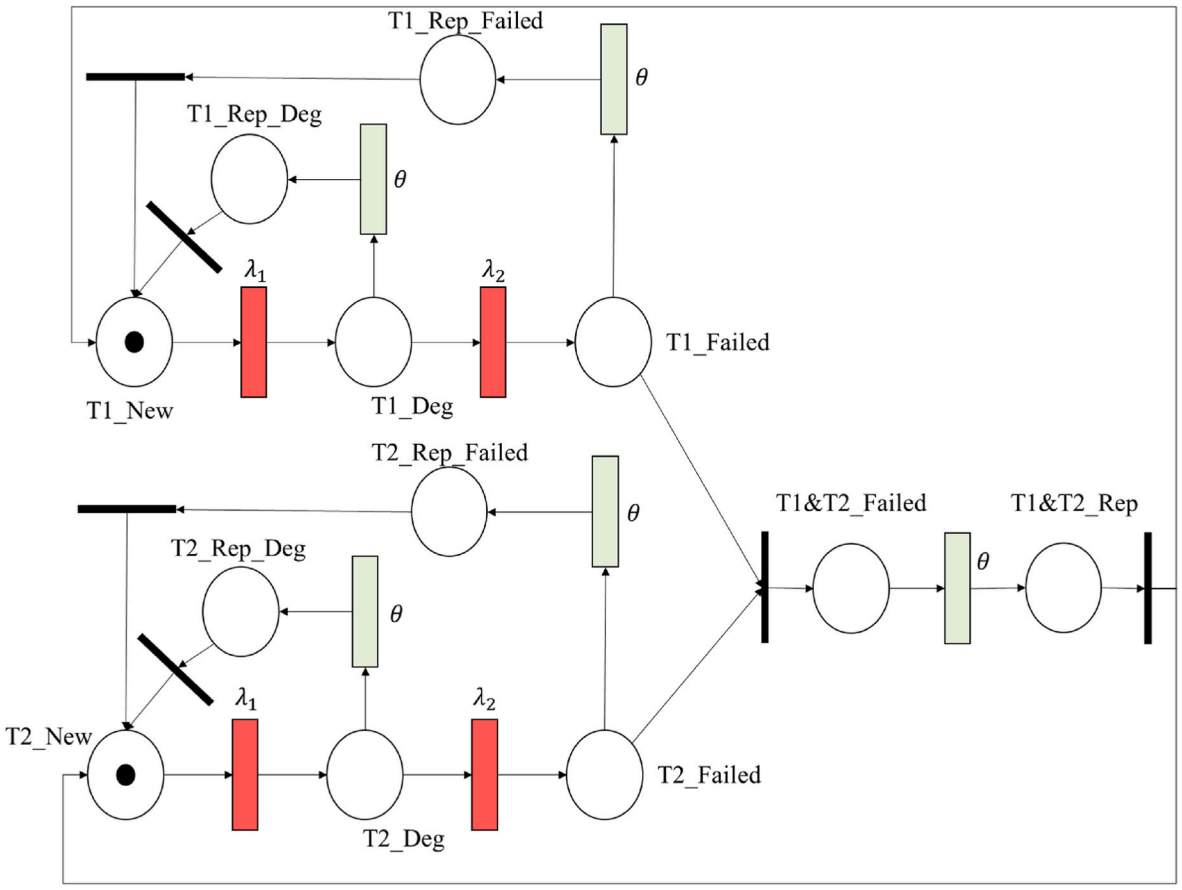


Fig. 8. Simplified Petri Net of the water supply dependency group during the standby phase.

Table 3
Probabilities of the water supplies of being in one of their states during the standby phase.

State	Probability
T1_New	0.957521532
T1_Deg	0.032277467
T1_Failed|T2_New or T2_Deg	0.010025367
T2_New	0.957521532
T2_Deg	0.032277467
T2_Failed|T1_New or T1_Deg	0.010025367
T1&T2_failed	0.000175633

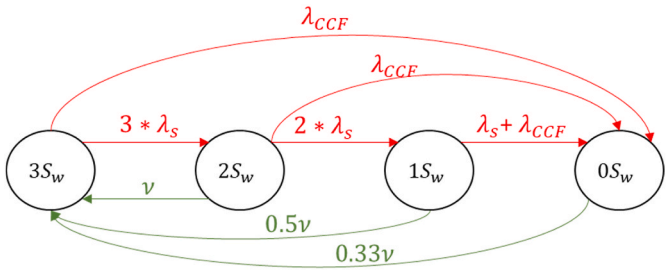


Fig. 9. Markov model of the pressure sensors during the standby phase.

From a theoretical perspective, this paper further proved the applicability of the D^2T^2 method through the application to a different case study, demonstrating the generalised capabilities of the algorithm. It extends the previous work by Tolo and Andrews (Andrews and Tolo, 2023) by implementing amendments to enable the application of the

Table 4
Probability of the pressure sensor system of being in one of the four states during the standby phase.

State	Probability
3Sw	0.999955001
2Sw	0.000029998
1Sw	0.000000001
0Sw	0.000015000

D^2T^2 algorithm to a safety barrier. Most of the safety barriers require an availability analysis and a reliability analysis for the standby phase and operational phase respectively. This aspect has led to the development of different dependency groups and modelling for the two phases.

This work has also relevant practical and managerial implications. Indeed, practitioners could employ the method to estimate the probability of failure of a safety barrier without typical limitations of the traditional FT analysis methods, leading to more representative results.

As any other works, this study conceal some limitations. For instance, influencing factors are not considered. Future studies may include the influencing factors through the integration of Bayesian Network into the D^2T^2 framework. Adding influencing factors allows to have a more realistic modelling of complex systems. It is also worth noting that defining a FT, along with PNs and Markov models, may represent a burden for inexperienced engineers. This factor hinders the adoption of the D^2T^2 algorithm. It follows that future studies can investigate the automatic generation of FT, PNs, and Markov models to ease and support the implementation of the D^2T^2 approach. Finally, while some data were extracted from literature, others were based on expert judgements. Therefore, future studies may integrate real-world

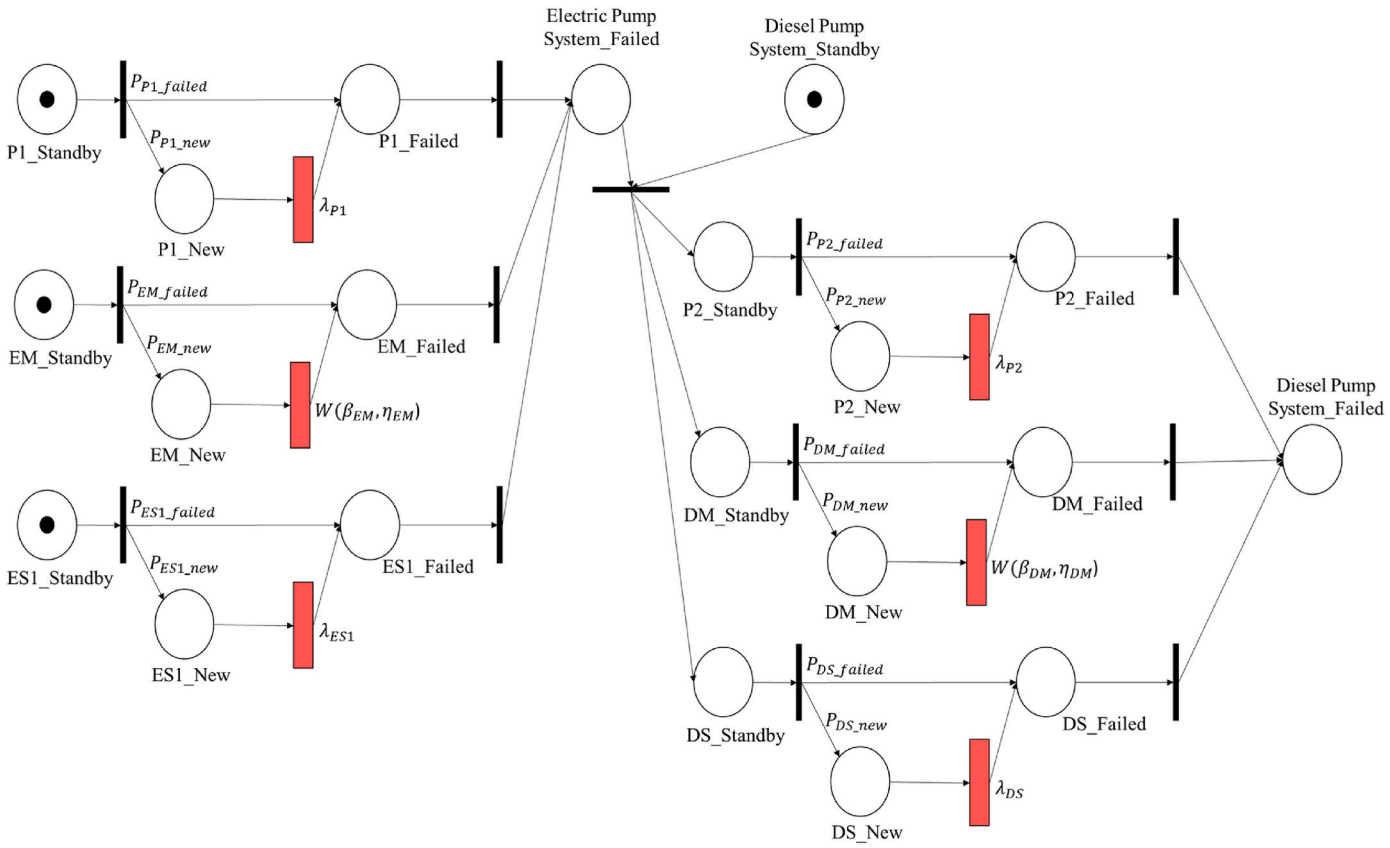


Fig. 10. Petri Net of the pump system dependency group during the operating phase.

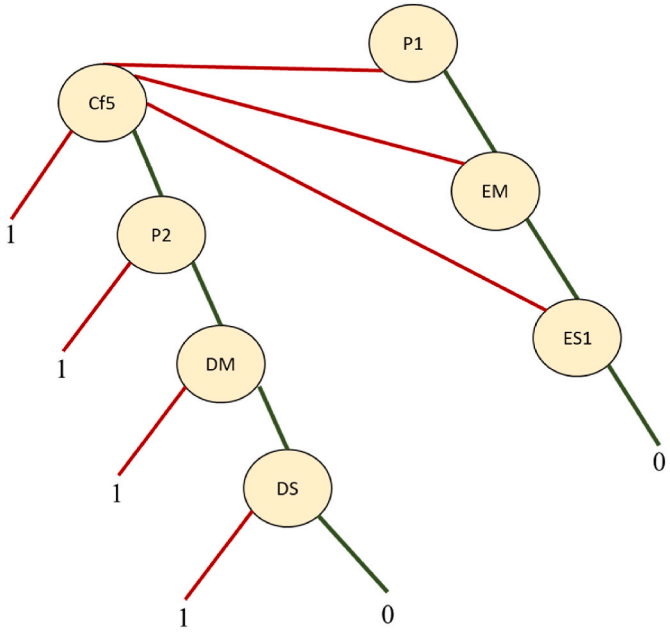


Fig. 11. Obtained BDD for the developed FT.

data to obtain more practical insights on the considered case study.

CRediT authorship contribution statement

Leonardo Leoni: Writing – review & editing, Writing – original draft, Validation, Methodology, Investigation, Formal analysis, Data curation. **John Andrews:** Writing – review & editing, Validation, Supervision, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Filippo De Carlo:** Writing – review & editing, Validation, Supervision, Methodology, Investigation, Formal analysis, Data curation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

John Andrews involvement in 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.

Data availability

Data are within the text

References

Akers, 1978. Binary decision diagrams. IEEE Trans. Comput. 100, 509–516.
Akyuz, E., Arslan, O., Turan, O., 2020. Application of fuzzy logic to fault tree and event tree analysis of the risk for cargo liquefaction on board ship. Appl. Ocean Res. 101, 102238.
Andrews, J., Tolo, S., 2023. Dynamic and dependent tree theory (D2T2): a framework for the analysis of fault trees with dependent basic events. Reliab. Eng. Syst. Saf. 230, 108959.
Andrews, J.D., Dugan, J.B., 1999. Dependency modeling using fault tree analysis. In: Proceedings of the 17th International System Safety Conference.

Andrews: Reliability and risk assessment - Google Scholar [WWW Document], n.d. URL https://scholar.google.com/scholar_lookup?title=Reliability%20and%20risk%20assessment&author=J.D.%20Andrews&publication_year=2002 (accessed 8.29.23).
Aslansefat, K., Kabir, S., Gheraibia, Y., Papadopoulos, Y., 2020. Dynamic Fault Tree Analysis: State-Of-The-Art in Modeling, Analysis, and Tools.
Badida, P., Balasubramaniam, Y., Jayaprakash, J., 2019. Risk evaluation of oil and natural gas pipelines due to natural hazards using fuzzy fault tree analysis. J. Nat. Gas Sci. Eng. 66, 284–292.
Bougofa, M., Bouafia, A., Chakhrit, A., Guetarni, I.H.M., Baziz, A., Aberkane, S., Zerouali, B., Kharzi, R., Bellaouar, A., 2022. Dynamic availability assessment using dynamic evidential Network: water deluge system case study. In: IOP Conference Series: Earth and Environmental Science. IOP Publishing, 012015.
Bucelli, M., Landucci, G., Haugen, S., Paltrinieri, N., Cozzani, V., 2018. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. Ocean Eng 158, 171–185.
Do, P., Voisin, A., Levrat, E., Iung, B., 2015. A proactive condition-based maintenance strategy with both perfect and imperfect maintenance actions. Reliab. Eng. Syst. Saf. 133, 22–32.
Dugan, J.B., Venkataraman, B., Gulati, R., 1997. DIFTree: a software package for the analysis of dynamic fault tree models. In: Annual Reliability and Maintainability Symposium. IEEE, pp. 64–70.
Dutuit, Y., Rauzy, A., 1996. A linear-time algorithm to find modules of fault trees. IEEE Trans. Reliab. 45, 422–425.
Elusakin, T., Shafiee, M., 2020. Reliability analysis of subsea blowout preventers with condition-based maintenance using stochastic Petri nets. J. Loss Prev. Process. Ind. 63, 104026.
Guetarni, I.H., Aissani, N., Châtelet, E., Lounis, Z., 2019. Reliability analysis by mapping probabilistic importance factors into bayesian belief networks for making decision in water deluge system. Process Saf. Prog. 38, e12011.
Hong, H.-P., Zhou, W., Zhang, S., Ye, W., 2014. Optimal condition-based maintenance decisions for systems with dependent stochastic degradation of components. Reliab. Eng. Syst. Saf. 121, 276–288.
Ikwan, F., Sanders, D., Hassan, M., 2021. Safety evaluation of leak in a storage tank using fault tree analysis and risk matrix analysis. J. Loss Prev. Process. Ind. 73, 104597.
Jafarian, E., Rezvani, M.A., 2012. Application of fuzzy fault tree analysis for evaluation of railway safety risks: an evaluation of root causes for passenger train derailment. Proc. Inst. Mech. Eng. - Part F J. Rail Rapid Transit 226, 14–25.
Jung, S., Yoo, J., Lee, Y.-J., 2020. A software fault tree analysis technique for formal requirement specifications of nuclear reactor protection systems. Reliab. Eng. Syst. Saf. 203, 107064.
Kabir, S., 2017. An overview of fault tree analysis and its application in model based dependability analysis. Expert Syst. Appl. 77, 114–135.
Kaiser, B., Gramlich, C., Förster, M., 2007. State/event fault trees—a safety analysis model for software-controlled systems. Reliab. Eng. Syst. Saf. 92, 1521–1537.
Kuzu, A.C., Akyuz, E., Arslan, O., 2019. Application of fuzzy fault tree analysis (FFTA) to maritime industry: a risk analysing of ship mooring operation. Ocean Eng 179, 128–134.
Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab. Eng. Syst. Saf. 143, 30–43.
Lavasani, S.M., Zendegani, A., Celik, M., 2015. An extension to Fuzzy Fault Tree Analysis (FFTA) application in petrochemical process industry. Process Saf. Environ. Prot. 93, 75–88.
Leoni, L., De Carlo, F., Abaei, M.M., BahooToroody, A., 2022. A hierarchical Bayesian regression framework for enabling online reliability estimation and condition-based maintenance through accelerated testing. Comput. Ind. 139, 103645.
Liaw, H.-J., Liu, C.-C., Wan, J.-F., Tzou, T.-L., 2023. Process safety management lessons learned from a fire and explosion accident caused by a liquefied petroleum gas leak in an aromatics reforming unit in Taiwan. J. Loss Prev. Process. Ind. 83, 105058.
Liu, Y., 2020. Safety barriers: research advances and new thoughts on theory, engineering and management. J. Loss Prev. Process. Ind. 67, 104260.
Mahmood, Y.A., Ahmadi, A., Verma, A.K., Srividya, A., Kumar, U., 2013. Fuzzy fault tree analysis: a review of concept and application. Int. J. Syst. Assur. Eng. Manag. 4, 19–32.
Mentes, A., Helvacioglu, I.H., 2011. An application of fuzzy fault tree analysis for spread mooring systems. Ocean Eng 38, 285–294.
Meshkat, L., Dugan, J.B., Andrews, J.D., 2000. Analysis of safety systems with on-demand and dynamic failure modes. In: Annual Reliability and Maintainability Symposium. 2000 Proceedings. International Symposium on Product Quality and Integrity (Cat. No. 00CH37055). IEEE, pp. 14–21.
Pan, J.-N., 1998. Reliability prediction of imperfect switching systems subject to Weibull failures. Comput. Ind. Eng. 34, 481–492.
Platz, O., Olsen, J.V., 1976. FAUNET: a program package for evaluation of fault trees and networks. Res. Establ. Riso. Report No 348, DK-4000 Roskilde, Denmark, Sept.
Purba, J.H., Lu, J., Zhang, G., Ruan, D., 2011. Failure possibilities for nuclear safety assessment by fault tree analysis. Int. J. Nucl. Knowl. Manag. 5, 162–177.
Ramezani, Z., Latif-Shabgahi, G.R., Khajeie, P., Aslansefat, K., 2016. Hierarchical steady-state availability evaluation of dynamic fault trees through equal Markov model. In: 2016 24th Iranian Conference on Electrical Engineering (ICEE). IEEE, pp. 1848–1854.
Ramzali, N., Lavasani, M.R.M., Ghodousi, J., 2015. Safety barriers analysis of offshore drilling system by employing Fuzzy Event Tree Analysis. Saf. Sci. 78, 49–59.
Ruijters, E., Stoelinga, M., 2015. Fault tree analysis: a survey of the state-of-the-art in modeling, analysis and tools. Comput. Sci. Rev. 15, 29–62.
Talebberrouane, M., Khan, F., Lounis, Z., 2016. Availability analysis of safety critical systems using advanced fault tree and stochastic Petri net formalisms. J. Loss Prev. Process. Ind. 44, 193–203.
Tolo, S., Andrews, J., 2022. An integrated modelling framework for complex systems safety analysis. Qual. Reliab. Eng. Int. 38, 4330–4350. https://doi.org/10.1002/qre.3212.
Wang, C., Wang, L., Su, C., Jiang, M., Li, Z., Deng, J., 2024. Modeling and performance analysis of emergency response process for hydrogen leakage and explosion accidents. J. Loss Prev. Process. Ind. 87, 105239.
Watson, H.A., 1961. Launch control safety study. Bell Telephone Laboratories. Murray Hill, N.J., USA.
Wu, J., Yan, S., Xie, L., 2011. Reliability analysis method of a solar array by using fault tree analysis and fuzzy reasoning Petri net. Acta Astronaut. 69, 960–968.
Yazdi, M., Mohammadpour, J., Li, H., Huang, H.-Z., Zarei, E., Pirbalouti, R.G., Adumene, S., 2023. Fault tree analysis improvements: a bibliometric analysis and literature review. Qual. Reliab. Eng. Int.
Yevkin, O., 2016. An efficient approximate Markov chain method in dynamic fault tree analysis. Qual. Reliab. Eng. Int. 32, 1509–1520.
Yuhua, D., Datao, Y., 2005. Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis. J. Loss Prev. Process. Ind. 18, 83–88.
Zhang, Q., Zhuang, Y., Wei, Y., Jiang, H., Yang, H., 2020. Railway safety risk assessment and control optimization method based on FTA-FPN: a case study of Chinese high-speed railway station. J. Adv. Transp. 2020, 1–11.
Zhang, X., Miao, Q., Fan, X., Wang, D., 2009. Dynamic fault tree analysis based on Petri nets. In: 2009 8th International Conference on Reliability, Maintainability and Safety. IEEE, pp. 138–142.
Zhou, J., Reniers, G., 2020. Modeling and application of risk assessment considering veto factors using fuzzy Petri nets. J. Loss Prev. Process. Ind. 67, 104216.
Zhu, C., Zhang, T., 2022. A review on the realization methods of dynamic fault tree. Qual. Reliab. Eng. Int. 38, 3233–3251. https://doi.org/10.1002/qre.3139.