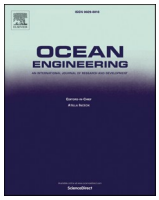
Ocean Engineering 237 (2021) 109653

Contents lists available at ScienceDirect

Ocean Engineering

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



Dynamic probabilistic risk assessment of decision-making in emergencies for complex systems, case study: Dynamic positioning drilling unit☆

Tarannom Parhizkar [a,b,c,*], Ingrid Bouwer Utne [a], Jan Erik Vinnem [a], Ali Mosleh [b,c]

[a] Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway
[b] The B. John Garrick Institute for the Risk Sciences, University of California, Los Angeles, USA
[c] Department of Materials Science & Engineering, University of California, Los Angeles, USA

ARTICLE INFO

Keywords:
Dynamic probabilistic risk assessment
Complex systems
Human-machine interaction
Decision making
Response time model
Bayesian network
Monte Carlo method
Dynamic event tree
Dynamic positioning system

ABSTRACT

Decision-making in emergency situations is a risky and uncertain process due to the limited information and lack of time. Some key problem parameters, such as the time required to complete important response tasks, must be estimated and are therefore prone to errors. Other parameters, such as the probability of occurrence of a consequential event, will typically change as the response operation progresses. As a result, there should be a dynamic probabilistic risk assessment framework to assess the risk level of decision scenarios and facilitate the decision-making process.

In this paper, a methodology for dynamic probabilistic risk assessment of decision making in emergencies for complex marine systems is proposed. In this method, a dynamic event sequence diagram is introduced that helps to quantify events probabilities as a function of time, as well as environmental and operational variables, considering events interdependencies and uncertainties. In addition, the effects of time required[1] and time available[2] for performing a decision in emergency are considered in the risk model. In this methodology, probabilistic models including Bayesian network and Monte Carlo simulation are utilized to quantify the uncertain behavior of the decision-making process in complex marine systems.

A computational study is also conducted to evaluate the methodology performance, in terms of effectiveness and efficiency. Computational results show that the proposed approach can obtain optimal solutions for large and practical problem sizes.

1. Introduction

Industrial accidents may cause losses of life or injury, social and economic disorders, or environmental pollution. When an incident occurs, the relevant decision makers need to decide what actions to take instantly to mitigate or minimize the potential negative effects. In most cases, the decision-making process in incidents, especially in emergency cases,[3] are complicated due to the limited time and information. As time passes, more information may become available; however, the consequences of the incident would be worse. Therefore, having more information about system health status and risk level of decision-making process at the early stages is an important research topic in complex systems.

In many risk assessment and management studies, the main focus is on the static risk, i.e., the risk and safety level of different scenarios without considering the dynamic nature of the system (Zhang et al., 2017) (Norazahar et al., 2017). Over the past decades, studies have been conducted to deal with dynamic risk assessment problems. Often, dynamic event trees connected to fault trees/BNs are used to analyze the dynamic behavior of complex systems in the risk assessment process (Hakobyan et al., 2008; Barua et al., 2020; Zhang et al., 2018; Kanes

☆ Initial emergency operations.

* Corresponding author. Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway.
E-mail addresses: tparhizkar@ucla.edu, Parhizkar.t@gmail.com (T. Parhizkar).

[1] Time required refers to the time needed to perform each level of decision-making process (detection, diagnosis, decision-making, execution).

[2] Time available is the time remaining before an accident happens in a system. It is derived from the dynamic simulator of the system. The dynamic simulator calculates the time remaining before a collision based on the system components status, operation and environmental conditions at the time of incident.

[3] An emergency case or situation is an unplanned or imminent event that affects or threatens the health, safety or welfare of people, property and infrastructure, and which requires a significant and coordinated response. The defining characteristic of an emergency event or situation is that usual resources are overwhelmed or have the potential to be overwhelmed.

https://doi.org/10.1016/j.oceaneng.2021.109653
Received 17 May 2021; Received in revised form 5 July 2021; Accepted 7 August 2021
Available online 17 August 2021

Table of nomenclature

Symbol	Description
α	Shape parameter
β	Inverse scale parameter
at_i	Time allocated to Event (i)
BN	Bayesian Network
CP	Conditional probability
HEP	Human error probability
K_p	Modified Bessel function
m	SPAR-H multiplier
P_i	Probability of Event (i)
$P_{i-(i+1)}$	Connection probability between Event (i) and events Event (i+1)
PSF	Performance shaping factor
RT	Response time
t_i	Occurrence time for Event (i)
t^*	Time required for Event (i)

et al., 2017; Meng et al., 2019; Li et al., 2019a, 2019b; Norazahar et al., 2018). Devooght et al. (Devooght and Smidts, 1996) were among the first pioneers that presented the dynamic event tree method. Tombuyses et al. (1998) and Kloos et al. (Kloos and Peschke, 2006) coupled the dynamic event tree method with Monte Carlo simulation for dynamic reliability problems.

Bi et al. (Bi and Si, 2012) proposed a dynamic risk model based on the Master Logic Diagram (MLD) for an oil spill scenario. Events in the MLD diagram are valued based on the simulation results. This diagram is used to identify the consequence contributors of an oil spill scenario, which was then tracked and grouped into classes, including environmental damage, asset loss, health impact, social effect and their contributing individual events in the bottom hierarchy of the MLD. Other methods include Go-Flow (Matsuoka and Kobayashi, 1988), Dynamic Flow Methodology (DFM) (Yau and Guarro, 1996), and dynamic simulation of the complex system coupled with a risk assessment model (Cojazzi, 1996; Izquierdo and Labeau, 2004; Vorobyev and Kudinov, 2011). For instance, Wang et al. (2016) proposed a dynamic risk assessment method for chemical processes. The model is updated continuously by monitoring key variables in a process. In addition, the consequences are estimated using dynamic loss functions considering multiple key state variables.

One of the main risk elements in risk assessment of decision-making process is human factors. In (Boring and Gertman, 2016), principles of human reliability analysis and quantification are presented; and in (Kolaczkowski, 2005a) good practices for implementing these principles are discussed. The U.S. Nuclear Regulatory Commission (NRC) has developed a guideline for quantification of Human Reliability Analyses (HRAs) to support risk-informed regulatory decision-making (US Nuclear Regulatory Commission, 2006). In these studies, human reliability is analyzed using Bayesian Networks (BNs)/Fault Trees (FTs)/Event Trees (ETs) or Standardized Plant Analysis Risk-Human Reliability Analysis (SPAR-H) method. The SPAR-H method is used as a part of risk assessment in different applications ranging from nuclear power plants (Boring and Gertman, 2016) to fire accidents in complex systems (Lewis et al., 2010). SPAR-H method helps to quantify the effect of performance shaping factors on the Human Error Probability (HEP). One of the important performance shaping factors is the available time at the time of incident. In (Hogenboom et al., 2021), the importance of time in the risk of dynamic positioning operations has been pointed out by analyzing time using different methods. In this study, different interviews with dynamic positioning operators have been performed and results illustrate that the effects of time available and time should be considered in human reliability analysis. Having more information about the system health status and risk level could help operators to make better decisions in a shorter time, decreasing HEP significantly in emergency situations.

The time required[4] and time available[5] are two time-related factors that affect human error and probability and decision-making process during an incident. In real incidents, the decision-making and system response process needs some time to be performed, which is known as time required. In addition to time required, time available should be estimated and addressed in a decision-making risk model. If the time available far exceeds the time required and there are not multiple competing tasks, the estimated HEP is not expected to be strongly influenced by time. However, if there is not enough or barely enough time to act, the estimated HEP is expected to be quite high (Kolaczkowski, 2005b), which may lead to failure in the emergency decision-making. Available time could be evaluated using system dynamic simulation based on available sensor data at the time of incident (initial event); and the time required could be estimated based on human response time models.

Even though contributions have been proposed to define and consider time available and time required in the decision-making process (Murchison and Gilmore, 2018; Wreathall et al., 2003; Joe et al., 2015; Swain and Guttmann, 1983), there is no concrete quantification method for evaluating HEP as a function of time available and time required.

In addition, interdependencies among response time[6] of decision-making steps (detection, diagnosis, decision-making, and execution) is barely addressed. Decision-making steps are highly interdependent and response time of each step affect the other steps performance. Moreover, system operation is affected by decisions dynamically. As a result, to have an accurate decision-making model, the interactions among decision-making steps, as well as human machine interactions, should be considered in the modeling procedure. The interactions between system and human in a dynamic environment are considered in a study carried out by Chang et al. (Chang and Mosleh, 2007a, 2007b, 2007c, 2007d, 2007e).

The objective of the present study is to develop a decision-making risk assessment framework that considers the dynamic nature of decision-making steps and their interdependencies with considering time available and time required for each step. In the proposed framework, the probability of a scenario is calculated as a function of previous events' probabilities and occurrence time (Utne et al., 2011). The method is based on a Dynamic Event Sequence Diagram (DESD) that gets inputs from response time models and Bayesian networks in order to quantify the occurrence time and probability of each event, respectively. There are multiple alternative decision scenarios in an emergency situation with different risk levels. The novelties of the proposed dynamic probabilistic risk assessment method are the ability to:

- Calculate the decision-making failure probability as a function of time available and time required (operator response time), and other performance shaping factors.
- Consider human-machine interdependencies by updating time available for next decision-making events based on the current system and operator(s) status and operating conditions.

[4] Time required refers to the time needed to perform each level of decision-making process (detection, diagnosis, decision-making, execution).

[5] Time available is the time remaining before an accident happens in a system. It is derived from the dynamic simulator of the system. The dynamic simulator calculates the time remaining before a collision based on the system components status, operation and environmental conditions at the time of incident.

[6] In this study, the response time is equal to the time required to perform human related events.

- Use data-driven response time models to evaluate time required for all decision-making events including detection, diagnosis, decision-making, and execution.
- Consider environmental, system and human factors uncertainties using Bayesian Network models.
- Utilize the Monte Carlo method to model the stochastic behavior of variables such as operators' detection, diagnosis, decision-making, and execution response times.

The paper is organized as follows: Section 2 presents the general form of the proposed methodology. Section 3 models the operator(s) decision-making process in a Dynamic Positioning (DP) drilling unit as a case study.

In Section 4, an emergency situation is described and based on the developed model in Section 3, the probability of failure of decision-making process is evaluated. In this section, the effects of available time and incident complexity on the decision-making risk level is analyzed. Then, Section 5 discusses the outcomes and proposes future research directions. Finally, in Section 6, conclusions are presented.

2. Methodology

Different temporal orderings of events could potentially lead to different scenarios. As a result, it is crucial to know the allocated time available in an incident. According to the reviewed literature (Villa et al., 2016), current dynamic Event Sequence Diagrams (ESDs) can only handle time delays in this regard. However, this study extends the dynamic ESD framework to consider time allocated[7] to each event and update the following events accordingly.

Fig. 1 presents a dynamic event sequence diagram. As can be seen, there are different phases (phase i, phase i+1, etc.) defined based on time intervals. Phases include multiple event alternatives in a time interval, e.g., Event (i) represents an event that happens between time t_i and t_{i+1}. The probability of each event is denoted by P, i.e., the probability of Event (i) is P_i. The time allocated to each event is presented as *at*, i.e., the time allocated to Event (i) is at_i.

As presented in Fig. 1, the connections between events are probabilistic. According to the figure, after Event (i), two different events (Event $(i+1)_1$ and Event $(i+1)_2$), with different probabilities ($P_{i\text{-}(i+1)1}$, $P_{i\text{-}(i+1)2}$) can occur. These connection probabilities depend on the system's environmental and operating conditions (Parhizkar et al., 2020a; Parhizkar., Mosleh.), as well as time allocated to the previous events.

The "constraints" presented in the figure illustrates the environmental and operational conditions, system boundary, and requirements that affect connection probability quantifications.

Fig. 2 presents an event flow diagram of a decision-making process in an emergency. In this figure, different phases of the decision-making including detection, diagnosis, decision-making, and execution are presented. In each phase, there are various events that should be defined for the case under study. In Fig. 2, some event examples for different phases are presented.

The presented phases in Fig. 2 are:

- Detection: The first step of the decision-making process, presented as a first phase (column) in the event flow diagram (Fig. 2). This event presents that the initiating event should be detected first, then other steps of the decision making could be performed.
- Diagnosis: The next step is diagnosis that could be performed based on different methods, such as monitoring and/or communication. Each method could be presented as one or multiple events in the diagnosis column.
- Decision-making: After the diagnosis process, different scenarios of recovery are proposed and compared in this phase.
- Execution: The last step of the decision-making process is execution. Actions could be performed manually, automatically, or combined, which are presented in this phase.

In the proposed method, events convey two important types of information, i.e., probability and time. The probability of an event is the measure of the chance that the event will occur, and it depends on environmental and operational factors including technical, human, and organizational risk factors that should be defined based on the scope of the study. The event probability can be calculated using a BN that is presented in Fig. 3. Different BN structures could represent human behavior/error. In order to quantify a BN, conditional probabilities among all the nodes should be available. In this study, the structure of the BN is simplified to enable quantification of all conditional probabilities accurately. The affecting factors (Performance Shaping Factors (PSF)) on human behavior/error are determined according to (Whaley et al., 2011). In this study, it is assumed that PSF factors are independent.

In the Bayesian network, Bayes rule is utilized to quantify the child node (human behavior error in Fig. 3). In the bayes rule, we need the probability of parent nodes and conditional probabilities of each arc (connection between nodes) to quantify a child node.

The probabilities of the parent nodes of the BN (Fig. 3) are defined based on the available evidence such as sensor data, at the time of incident.

Conditional probabilities of the BN can be calculated based on SPAR-H method (Byeet al., 2017). SPAR-H method is a human reliability assessment tool that uses PSFs to quantify the probability of human error. PSFs are the aspects of human behavior and the environment that can affect human performance, such as stress, level of training, and task complexity. Based on this method, the HEP can be quantified using Eq. (1).

$$CP = \prod PSFs \tag{1}$$

When 3 or more negative PSF influences are present, in the equation above, the conditional probability should be computed as a composite PSF score used in conjunction with the adjustment factor. Negative PSFs are present anytime a multiplier greater than 1 is selected. The composite PSF score is computed by multiplying all the assigned PSF values. Then the adjustment factor below is applied to compute the conditional probabilities. The first term of the equation presents PSFs for human errors related to the diagnosis tasks (e.g., detection, diagnosis, making a decision) and the second term is PSFs of human errors related to action tasks (e.g., execution), (Groth and Swiler, 2012).

$$CP = \frac{0.01 \times \prod PSFs}{0.01 \times (\prod PSFs - 1) + 1} + \frac{0.001 \times \prod PSFs}{0.001 \times (\prod PSFs - 1) + 1} \tag{2}$$

where, 0.01 and 0.001 are nominal human error probabilities for detection/diagnosis and action/execution tasks, respectively. These numbers are derived based on several studies on human behavior and human error quantifications (Byeet al., 2017). PSFs are multipliers of each parent node that impact the human performance. These values are highly dependent on the type of event and their values could be found in related references. (Byeet al., 2017) has presented PSFs for operator(s) on board in a dynamic positioning drilling unit. For instance, for stress PSF factor, there are three SPAR-H levels as follow that can be used to quantify stress PSF at different situations.

Extreme: A level of disruptive stress in which the performance of most people will deteriorate drastically. This is likely to occur when the onset of the stressor is sudden, and the stressing situation persists for long periods. This level is also associated with the feeling of threat to one's physical well-being or to one's self-esteem or professional status and is qualitatively different from lesser degrees of high stress (e.g.,

[7] Time allocated is the time spent on an event. When there is a sufficient time, time allocated to each event is equal to the time required.

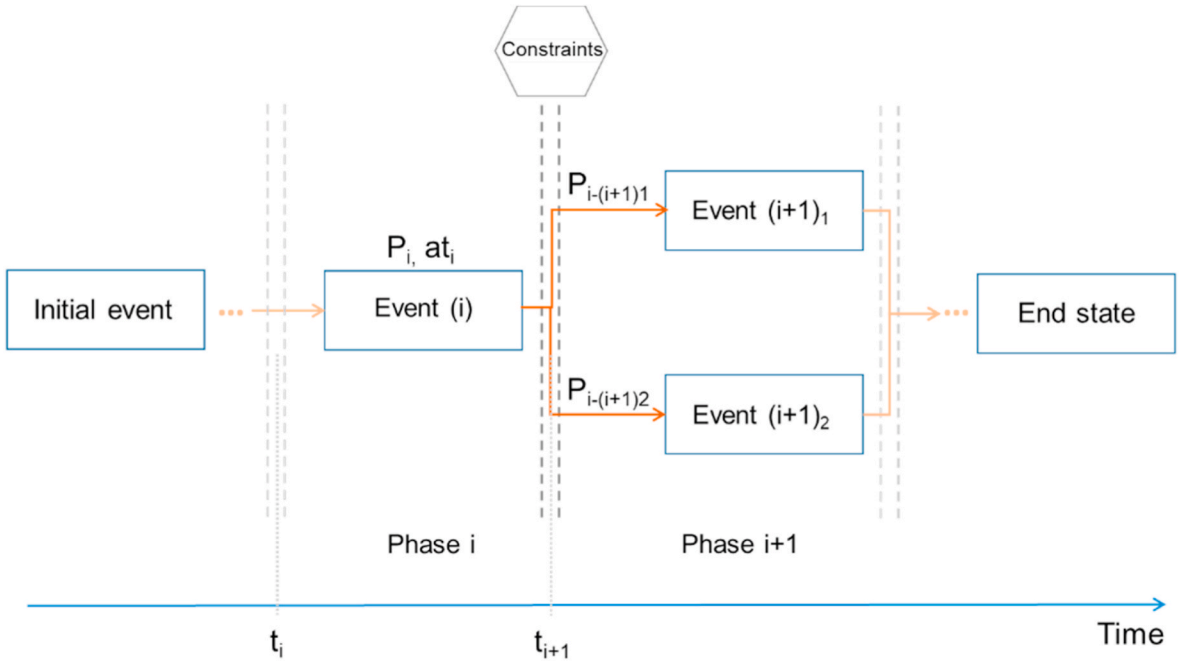


Fig. 1. Dynamic event sequence diagram example.

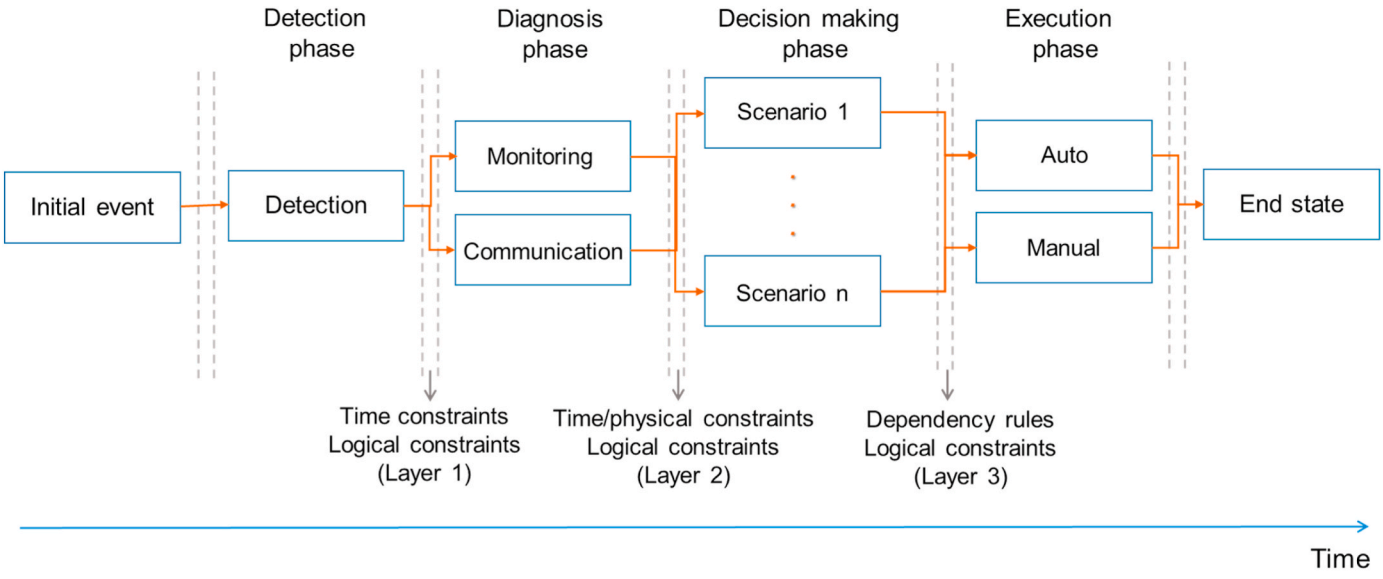


Fig. 2. Dynamic event sequence diagram of decision-making in emergency.

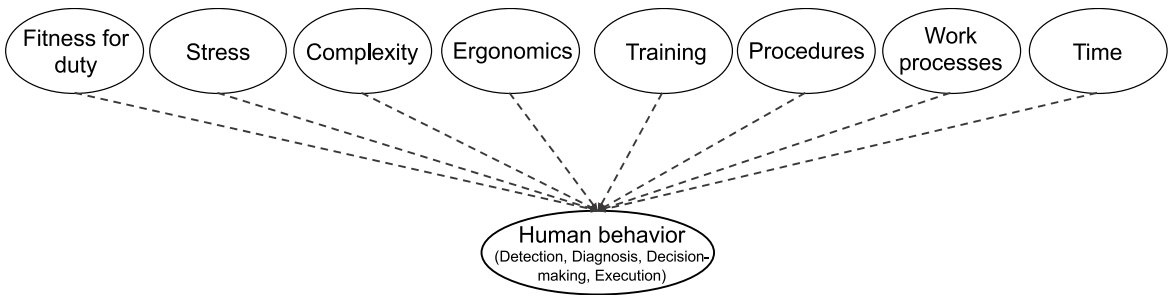


Fig. 3. Bayesian network of human behavior events (Detection, Diagnosis, Decision-making, Execution) presented in Fig. 2.

catastrophic failures can result in extreme stress for operating personnel because of the potential for radioactive release). In this situation the stress PSF factor is equal to 25, (Byeet al., 2017).

High: a level of stress higher than the nominal level (e.g., multiple instruments and annunciators alarm unexpectedly and at the same time; loud, continuous noise impact's ability to focus attention on the task; the consequences of the task represent a threat to facility safety). In this situation the stress PSF factor is equal to 5, (Byeet al., 2017).

Nominal: The level of stress that is conducive to good performance. In this situation the stress PSF factor is equal to 1, (Byeet al., 2017).

For other PSFs such as fitness for duty, complexity, ergonomics, etc. there are different categories and PSF values accordingly. The PSF values are used in Eqs. (1) and (2) to quantify conditional probabilities of each parent nodes.

These conditional probabilities as well as parent nodes' probabilities are taken as inputs in Bayes rules in the Bayesian network to calculate the human behavior (child node) probability. The human behavior node could particularly model the detection (Section 3.1), diagnosis (Section 3.2), decision-making (Section 3.3), and execution processes (Section 3.4).

One of the main innovations of the proposed methodology is in the quantification process of conditional probability of the "Time" node. The time refers to the time allocated to the event. The conditional probability as a function of the time allocated to an event could follow different patterns. In this study, a linear function based on the SPAR-H method principles is proposed.

In SPAR-H method, the failure probability of an event (diagnosis or action tasks) is calculated using Eqs. (1) and (2), (Byeet al., 2017). Table 1 presents the SPAR-H multiplier (presented as PSFs in Eqs. (1) and (2)) and event probabilities for four different allocated times (Byeet al., 2017).

The values in the table give four probabilities at four different allocated times (red dots presented in Fig. 4). In order to make the conditional probability function continuous, it is assumed that the function follows a linear pattern at the other allocated times, as presented in Fig. 4.

The functions of linear lines between dots could be calculated based on the time required and time allocated to the tasks. For instance, for diagnostic tasks, the linear functions could be calculated as Eqs. (3)–(6).

$$CP_{time} = \frac{(1-0.3355)}{t^*/3} \times at \; at < \frac{1}{3} \times t^* \tag{3}$$

Table 1
SPAR-H time multipliers and probabilities for four allocated time (Byeet al., 2017).

SPAR-H levels	m SPAR-H multipliers	$1-(Pd)_i$ Diagnosis task failure	$1-(Pd)_i$ Action task failure
Inadequate time: If the operator cannot diagnose the problem in the amount of time available, no matter what s/he does, then failure is certain.	-	1	1
Barely adequate time: 1/3 the average time required to diagnose the problem is available.	50	$\frac{0.01\times 50}{0.01\times 49+1} = 0.3355$	$\frac{0.001\times 50}{0.001\times 49+1}$
Barely adequate time: 2/3 the average time required to diagnose the problem is available.	10	$\frac{0.01\times 10}{0.01\times 9+1} = 0.0917$	$\frac{0.001\times 10}{0.001\times 9+1}$
Nominal time: on average, there is sufficient time to diagnose the problem.	1	0.01	0.001

$$CP_{time} = (1-0.3355) + \frac{(1-0.0917)-(1-0.3355)}{t^*} \times at \; \frac{1}{3} \times t^* < at < \frac{2}{3} \times t^* \tag{4}$$

$$CP_{time} = (1-0.0917) + \frac{(1-0.01)-(1-0.0917)}{t^*} \times at \; \frac{2}{3} \times t^* < at < t^* \tag{5}$$

$$CP_{time} = 1 - 0.01\, t^* < at \tag{6}$$

For action tasks, the constants of the linear equations, should be updated based on the numbers presented in Table 1. As can be seen, the linear functions depend on the time required (t*) and time allocated (at) to each task. In the case study section, these functions are updated according to the required time for each task.

The time allocated (at) to each event depends on the nature of the event. Events with a technical basis, such as automatic shutdown of a system, engine part load operation, etc. could have a specific time required that depends on the machinery limitations. However, there are other types of events with human interference, such as monitoring, diagnosis, execution, etc.; in these cases, time allocated is a function of various environmental, operational, and behavioral parameters such as experience, training, stress level, etc., and this creates parametric uncertainties that evolve in complexity as one moves from one complex emergency to another. The time allocated could be evaluated using data-driven probabilistic models. For instance, in (Hockley, 1984; Batur et al., 2018; Zandt, 2002) different distributions for human response time (allocated time) are proposed. For instance, a human response time could follow inverse gamma, lognormal, gamma or generalized gamma distributions. Operators allocate time to the remaining decision-making events based on the remaining time available. For instance, when there is enough time available (nominal time according to Table 1), recovery action could be performed. However, in situations with barely adequate time (defined in Table 1), emergency actions, such as emergency shutdown are performed to avoid accidents. At the time of incident, time available is derived from the dynamic simulator of the system. The dynamic simulator consists of dynamic models[8] of system components and calculates the time remaining before accident/failure based on the system components status, operation, and environmental conditions at the time of incident. As time passes, the time available decreases based on the time allocated to each event.

In the proposed methodology, the effect of remaining time on the upcoming decision-making events' probabilities are quantified using Eqs. (3)–(6). The derived conditional probabilities will be used as the conditional probabilities of the time node in the Bayesian network (Fig. 3). In addition, the conditional probabilities of other Bayesian network nodes such as fitness for duty, stress, complexity, etc. will be evaluated using Eqs. (1) and (2). All conditional probabilities will be used to quantify the child node (HEP) of the Bayesian network using Bayes rules. In the quantification process of the Bayesian network, it is assumed that parent nodes of the Bayesian network are independent.

Fig. 5 presents the flow diagram of the proposed methodology. In the response time model, the time allocated to each decision-making event is evaluated. The allocated times are used to calculate the conditional probability of the "Time" node based on Table 1 and Eqs. (3)–(6).

The dynamic simulator performs basic calculations to derive available time using sensor data. Sensor data include all data from different sensors installed in the system that are used to measure system operating conditions and performance such as temperature, pressure, mass flow rate, position, velocity, power, etc. the sensor data is used to estimate the available time before an accident. For instance, in a vessel, using sensors, the vessel velocity and its distance from an obstacle can be

[8] Dynamic models help understand the system behavior. These models are either from fundamental relationships (first principles, physics-based) or/and derived from data (empirical) that rely on knowledge of the process.

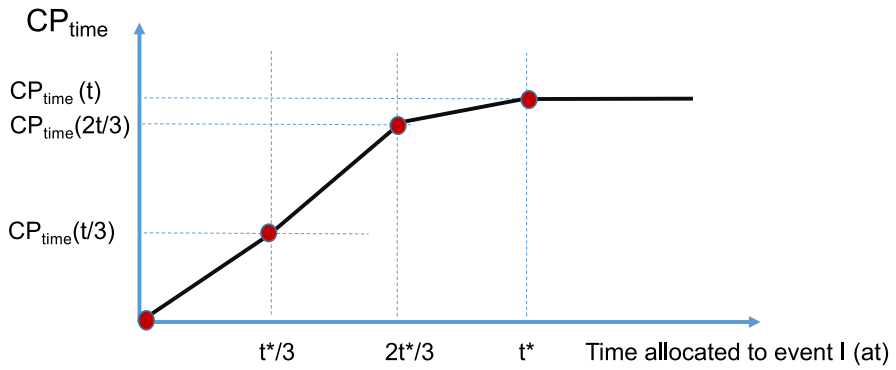


Fig. 4. "Time" node conditional probability as a function of time allocated for events with human involvement (t* is the time required for the event.).

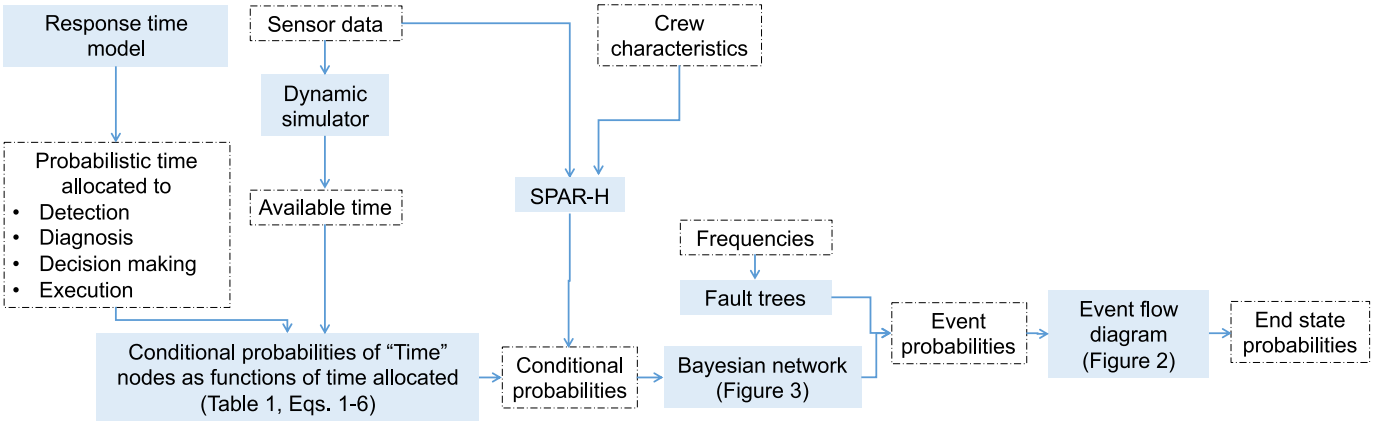


Fig. 5. Flow diagram of the proposed methodology based on Hybrid Causal Logic (HCL) methodology.

measures. In the vessel dynamic simulator, available time before collision is estimated using these sensor data. In addition to sensor data that can be used for available time calculation, crew characteristics are used in the SPAR-H model to calculate parent nodes' probabilities (PSF factors) of BNs. For instance, according to a crew member behavior, we can estimate the probability of fitness for duty, stress level, etc. of the crew member. These probabilities are used to calculate human error probability using the BN (Fig. 3).

In addition, the system under study could have technical components, such as engine, control system, etc. The failure/success probability of these technical components could be calculated using fault tree methods. The output of fault trees, in addition to human error

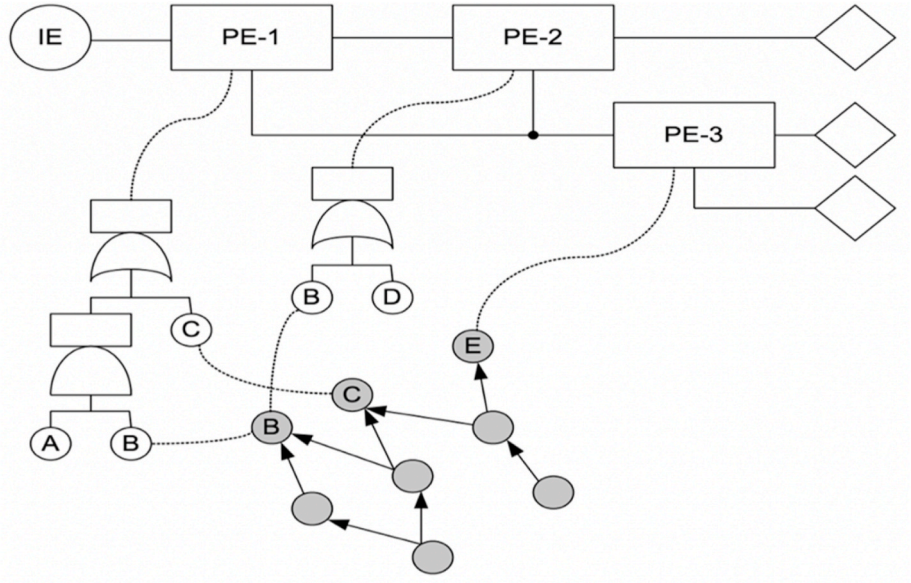


Fig. 6. Explicit coverage of complex interdependencies of risk events by HCL modeling technique.

probability, are used to calculate failure/success probabilities of the ESD events, and consequently to evaluate the probability of end states in the framework using Hybrid Causal Logic (HCL) methodology.

The HCL methodology contains algorithms that convert ETs and FTs into equivalent Binary Decision Diagrams (BDDs). A BDD is a rooted, directed, acyclic graph with an unconstrained number of in-edges and two out-edges – one for each two states (such as 'true' or 'false') of any given variable. A BDD is a binary decision tree over the Boolean variables where identical Boolean expressions are unified. Thus, a BDD has two terminal nodes labeled 0 (false) and 1 (true), representing the final value of the logical expression (Røed et al., 2009).

The HCL algorithm is a major extension of BDDs. The HCL layers of ESDs or ETs and FTs are included through transformation into BDDs and linked to the BNs layer by properly handling the dependencies (Wang, 2007). As we can see in Fig. 6, linking BNs to EDS and FT models provides a way for explicitly accounting for potentially complex and often hidden interdependencies of risk models elements. As an example, we note that basic events B and C which appear in different FTs of Fig. 6 are in fact interdependent as they are both linked to the same BN (of other risk factors).

The main outcome of the methodology (Fig. 5) is the probability of the end states of the presented ESD in Fig. 2. The end states could be system failure or success, and the methodology proposed in the paper evaluates the success/failure probabilities of the decision-making process in emergency situations.

As mentioned, the allocated time to each event is a stochastic variable and could take different values, depending on environmental, operational, and human characteristics. Therefore, there is not a single result for end state probabilities. A method to consider the stochastic behavior of allocated times is Monte Carlo (MC) method. MC is a class of computational algorithm that performs repeated random sampling. Samples are randomly selected from a distribution/dataset, then the samples are taken as model inputs, and results are generated accordingly. In the presented methodology (Fig. 5), samples could be randomly selected from response time distributions of each event (i.e., the samples include four random allocated times for detection, diagnosis, decision-making and execution process, derived from their response time distributions). Then, end state probabilities are calculated using the presented methodology in Fig. 5. The random sampling process is repeated for the predefined total number of MC simulations. The output of MC is a distribution of end state probabilities, presenting all model outputs for every samples. This is further exemplified in the next Section with a case study on a Dynamic Positioning (DP) system in a Mobile Offshore Drilling Rig Unit (MODU).

3. Case study

The proposed methodology is applied to a DP system in a MODU. The DP is a computer-controlled system used to automatically maintain a ship or vessel's position and heading by using its own propellers and thrusters. The studied DP system enables positioning of an offshore drilling unit. An offshore drilling unit operates in a green zone inside a yellow limit, presented in Fig. 7, (Chen et al., 2008). When an initiating event happens, the vessel loses the capability to maintain position and may enter the yellow zone. Whenever the vessel passes the yellow limit, the operation of the unit must be stopped, and the operator starts to prepare for disconnection. When the vessel passes the red limit, emergency disconnection must be initiated to disconnect the riser and shut in the well. Failure of disconnection may lead to damage of riser, blowout preventer or wellhead and hydrocarbon influx (kick), which can cause vessel downtime, significant financial losses and environmental damages.

The event flow diagram for the case study is presented in Fig. 8. As can be seen at the first level, the abnormalities should be detected. Then the operator starts monitoring to diagnose any undesired deviations in the system. In the decision-making stage, crews may share some knowledge-based information that could help them in the next step of making a decision. Then, one or some of the recovery tasks, i.e., change

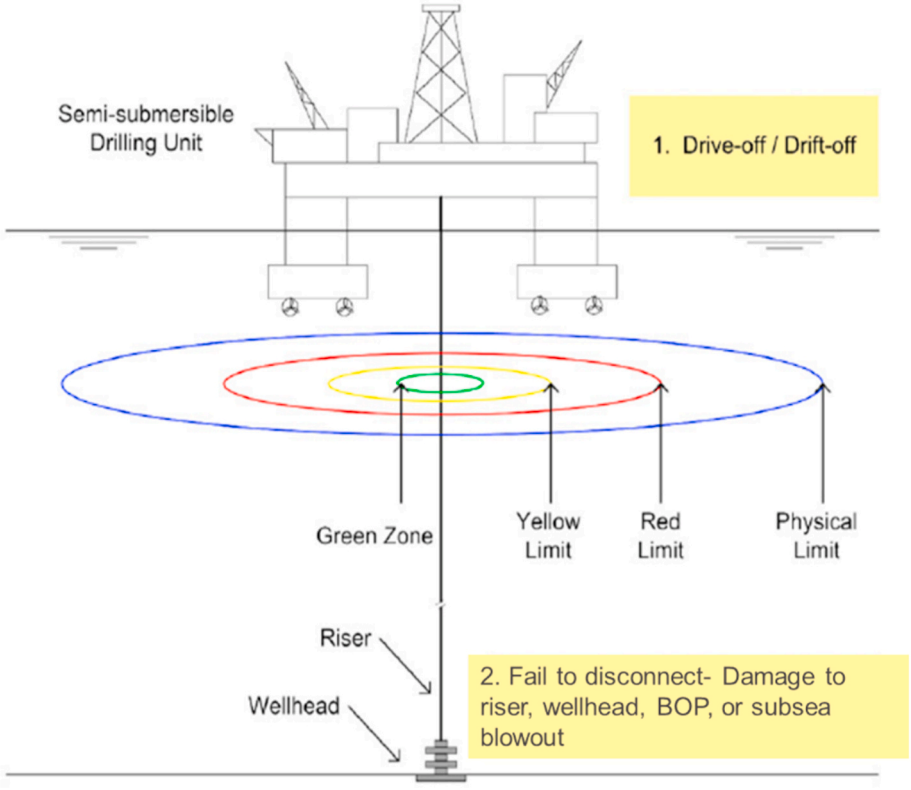


Fig. 7. DP drilling operation zones (Chen et al., 2008).

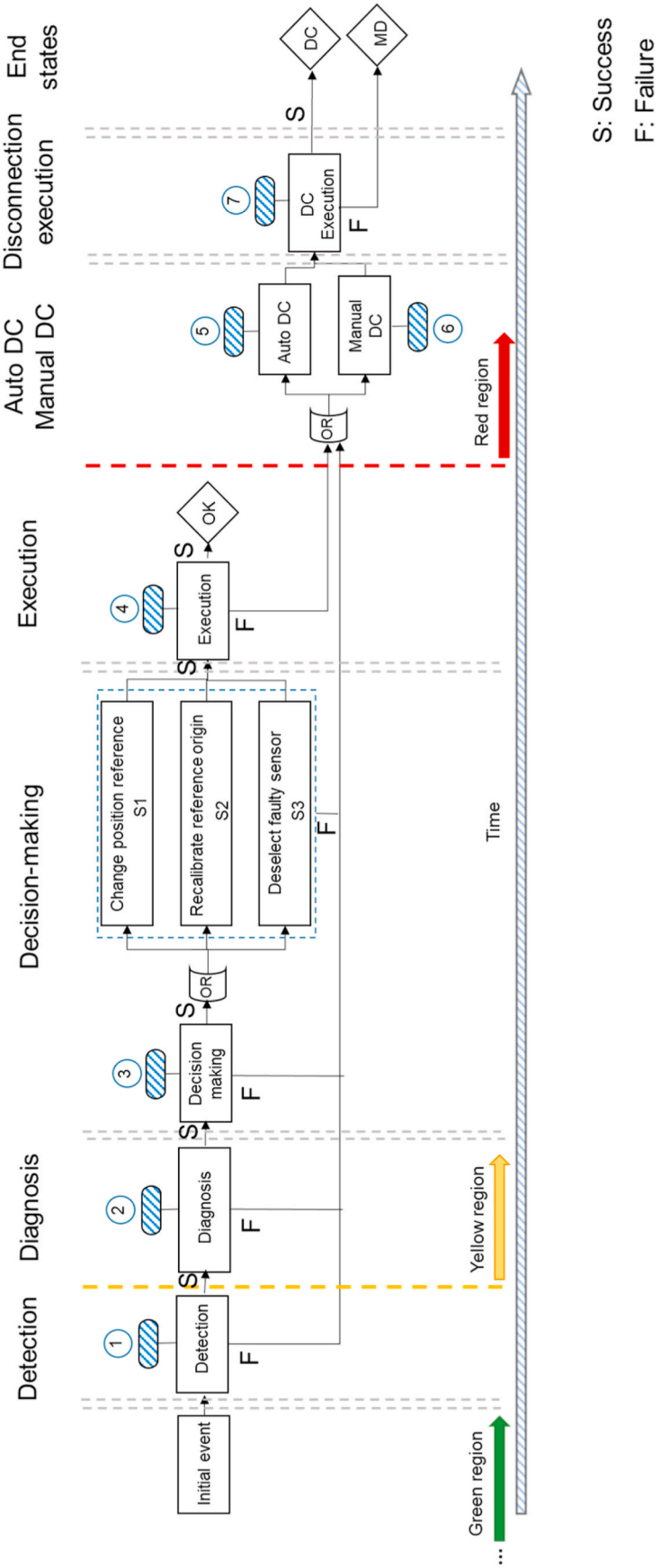


Fig. 8. Decision-making event flow of a DP drilling unit.

position reference, recalibrate reference origin, and deselect faulty sensor is to be executed. The formulated tasks are transformed into sequenced muscle movements, and the tasks are executed in the last stage. If any of the events fails, the drilling unit will pass the red limit; and the disconnection should be performed. Disconnection could be performed by the operator either manually or automatically. In both cases, there is a probability of failure; therefore, possible end states are DC (disconnect properly), MD (mechanical damage to due disconnection failure) and OK (system maintains position and returns to safe zone).

In auto and manual disconnection level, the failure of hardware, software, and human components are modeled using fault trees (Sections 3-5 and 3-6, respectively). The hardware components are the power system including power generation units, switches, UPS, and hardware parts of the control system computer. Software component includes the software parts of the control system computer. However, in all other levels (detection, diagnosis, decision-making, execution, and disconnection execution), it is assumed that there is no failure in hardware and software, and the only possible failure is due to human factors.

The next step is the quantification of events, which is presented in the following subsections for each event.

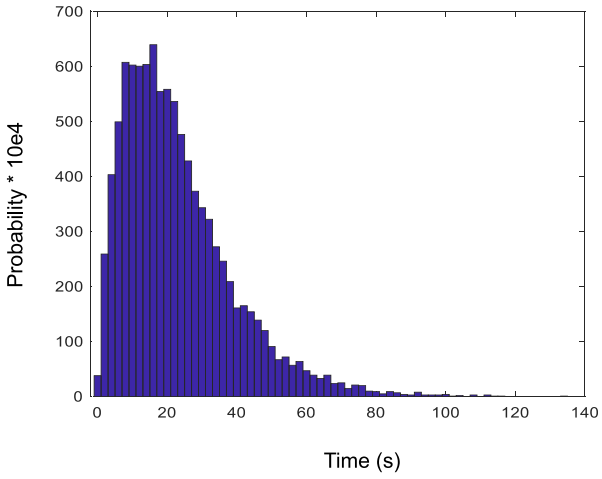


Fig. 10. RT (time allocated) distribution of the detection process.

3.1. Detection

At the first stage, the operator should detect deviations from normal operation (first phase/column presented in Fig. 8). The probability of detection $P_{detection}$ depends on time, fitness for duty, stress, complexity, ergonomics, training, and work processes; and could be calculated based on the BN presented in Fig. 9. The conditional probabilities of all parent nodes except "Time" are quantified using Eqs. (1) and (2), and the multipliers of each parent node are derived from (Byeet al., 2017).

The conditional probability of the "Time" node, i.e., allocated time to the detection, could be calculated based on Eqs. (3)–(6). According to (Byeet al., 2017), the detection of an initiating event in a DP drilling unit takes approximately 23 s. Therefore, based on Table 1 and Eqs. (3)–(6), the conditional probability function of the "Time" node for the detection event can be calculated.

According to the reviewed literature, the Response Time (RT) of operator(s)' detection follows the Gamma distribution (Palmer et al., 2011). The gamma distribution is a two-parameter category of the continuous probability distributions. Eq. (7) presents a general form of the gamma distribution. The gamma distribution can be parameterized in terms of a shape parameter α and an inverse scale parameter $\beta = 1/\theta$.

$$f(x;\alpha,\beta) = \frac{\beta^{\alpha} x^{\alpha-1} e^{-\beta x}}{\Gamma(\alpha)} \tag{7}$$

In (Palmer et al., 2011), it is shown that the best value for shape and scale parameters for the detection response time are 2 and 400, respectively. Fig. 10 presents the shape of the gamma distribution with these parameters, and the mean value of 23 s.

Based on the presented distribution, allocated time to the detection process can be estimated, and using the estimated allocated time, the conditional probability of the "Time" node for the detection event can be calculated (Eqs. (3)–(6)).

3.2. Diagnosis

In this step, the operator tries to diagnose failures and errors in the system by monitoring vessel screens and the environment (second phase/column presented in Fig. 8). After the detection of an initiating event, the DP operator monitors deviations based on the data perceived from one or several information sources, including alarm/event list, vessel position plot from the DP console, hydro acoustic position reference system screen, position reference system information from DP console, thruster output, power consumption, vibration of bridge and acoustic noise (depending on vessel size and bridge location). In addition, the DP operator(s) will actively search and process the information in order to perform failure diagnosis. Generally, according to these data, the DP operator(s) could determine likely failures and the severity of the situation.

The probability of diagnosis depends on multiple factors and could be calculated using the BN model, as presented in Fig. 11. The conditional probabilities of all the parent nodes, except the "Time" node are quantified using Eqs. (1) and (2), and the multipliers are derived from (Byeet al., 2017). Based on expert judgment, it is assumed that the highlighted nodes have the most impact. Thus, higher conditional probabilities are assigned to these nodes in comparison to other parent nodes.

The time required for the diagnosis process is about 20 s (Chen et al., 2008). Therefore, according to Table 1 and Eqs. (3)–(6), the conditional probability of the "Time" node could be calculated.

The time allocated to the diagnosis process is stochastic. According to (Ma et al., 2016), the best distribution that fits human response time is the generalized inverse gamma distribution. In probability theory and

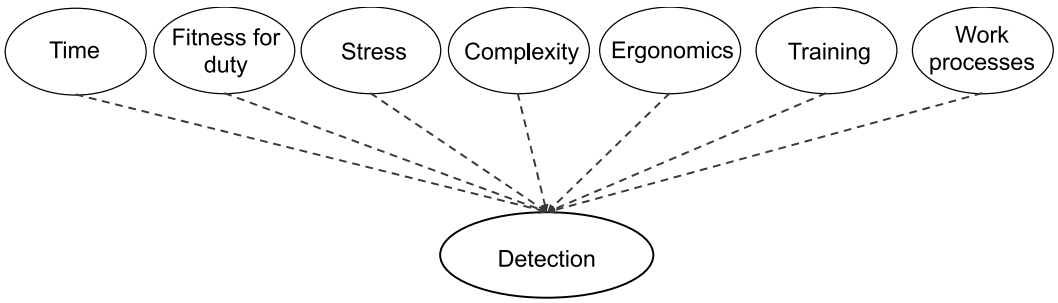


Fig. 9. The Bayesian network of detection probability.

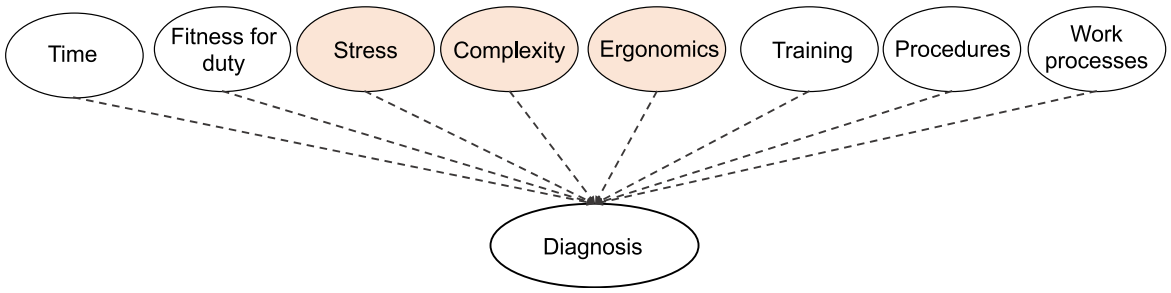


Fig. 11. Bayesian network of diagnosis probability.

statistics, the Generalized Inverse Gaussian distribution (GIG) is a three-parameter category of continuous probability distributions. The general form of the GIG distribution is presented in Eq. (8).

$$f(x) = \frac{(a/b)^{p/2}}{2K_p(\sqrt{ab})} x^{(p-1)} e^{-(ax+b/x)/2}, \quad x > 0, \tag{8}$$

Where, Kp is a modified Bessel function of the second kind, a >0, b > 0 and p are real parameters of the function. In this study, the time allocated to the diagnosis process is assumed to follow the GIG distribution. a, b and p are considered to be equal to 1, 1, −0.5 respectively. These factors give a narrow tail that shows that there are some diagnosis processes that may take longer time. In addition, these factors give the mean value of the distribution equal to 20 s, which is the average time required for the diagnosis process, according to (Chen et al., 2008).

Based on the presented distribution, allocated time to the diagnosis process can be estimated, and using the estimated allocated time, the conditional probability of the "Time" node for the diagnosis event can be calculated (Eqs. (3)–(6)).

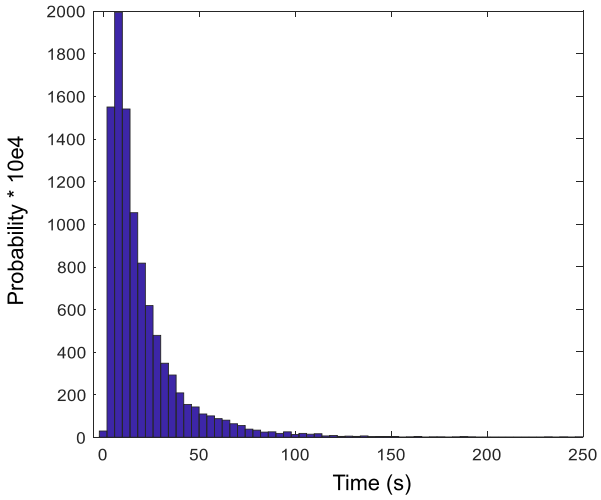


Fig. 12. RT (time allocated) distribution of the diagnosis process.

3.3. Decision-making

In this step, crews communicate and interact to understand the situation in a better way and to be able to make an appropriate decision in a short time (third phase/column presented in Fig. 8). Finally, the recovery tasks are concluded by an operator based on the gathered information and time and operational constraints. Three main decisions could be performed as recovery tasks in a DP drilling unit in short time (Chen et al., 2008).

1. Change position reference, i.e., deselect the faulty position reference and select an alternative position reference.
2. Recalibrate reference origin in DP control system.
3. Deselect faulty vessel sensor.

The probability of successful decision-making depends on multiple factors and could be calculated using the BN presented in Fig. 13. The conditional probabilities of all parent nodes, except the "Time" node are quantified using Eqs. (1) and (2) and the multipliers are derived from (Byeet al., 2017). Based on expert judgment, it is assumed that the highlighted red node has the most, and highlighted blue nodes have the least impact on successful decision-making process.

The decision-making process takes about 5 s (Chen et al., 2008); therefore, based on Table 1 and Eqs. (3)–(6), the conditional probability of the "Time" node for the decision-making event can be evaluated.

The time spent at this step follows the GIG distribution, as the diagnosis step. However, as the time required for this step is shorter than previous steps (Chen et al., 2008), a, b and p parameters are considered equal to 2, 1 and 0, respectively. Fig. 14 presents the GIG distribution for time allocated to the decision-making. The mean value of the distribution is equal to 5 s (Chen et al., 2008).

Based on the presented distribution, allocated time to the decision-making process can be estimated, and using the estimated allocated time, the conditional probability of the "Time" node for the decision-making event can be calculated (Eqs. (3)–(6)).

3.4. Execution

At this phase, the formulated recovery task from the previous step is executed (fourth phase/column presented in Fig. 8). The probability of execution depends on multiple factors, including time, fitness for duty, stress, ergonomics, training, and work processes and can be calculated using the BN presented in Fig. 15. The conditional probabilities of all parent nodes, except the "Time" node are quantified using Eqs. (1) and (2) and the multipliers are derived from (Byeet al., 2017).

The execution time process takes about 3 s (Chen et al., 2008); therefore, based on Table 1 and Eqs. (3)–(6), the conditional probability of the "Time" node for the execution event can be evaluated.

The response time of execution follows GIG distribution as in previous stages. However, as the time required for this step is shorter than previous ones, a, b and p parameters are considered equal to 2, 1 and 0, respectively, with 3 s mean value (Chen et al., 2008).

Based on the presented distribution, allocated time to the execution process can be estimated, and using the estimated allocated time, the conditional probability of the "Time" node for the execution event can be calculated (Eqs. (3)–(6)).

3.5. Auto DC

If the vessel movement could not be controlled, it will enter the red zone (fifth phase/column presented in Fig. 8). After entering the red zone, the vessel must be disconnected. Disconnection can be performed automatically or manually. The probability of auto disconnection mostly

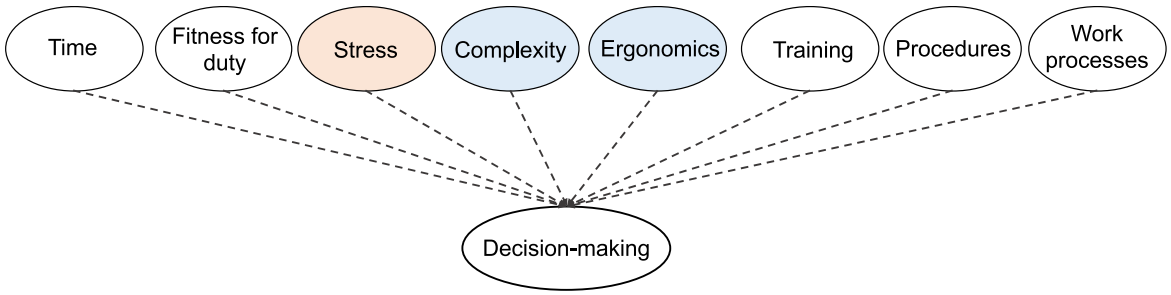


Fig. 13. Bayesian network of successful decision-making probability.

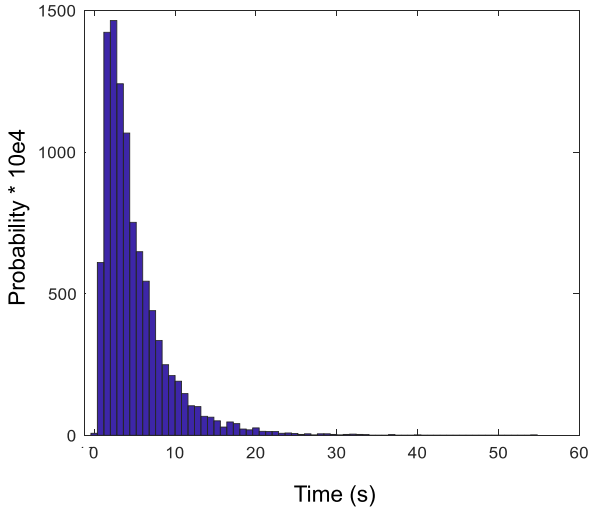


Fig. 14. RT (time allocated) distribution of the decision-making process.

depends on technical factors of the DP drilling unit and can be calculated using the fault tree presented in Fig. 17, (Parhizkar et al., 2020b). The frequencies of basic events are presented in (Parhizkar et al., 2020b).

3.6. Manual DC

Another option, after entering the red zone, is manual disconnection (fifth phase/column presented in Fig. 8). The probability of manual disconnection depends on technical and human factors. The related fault tree and BN of the manual disconnection is presented in Fig. 18 and Fig. 19, respectively, (Parhizkar et al., 2020b). The frequencies of the fault tree basic events are presented in (Parhizkar et al., 2020b).

As shown, one of the initial events of the fault tree is human error that could be quantified using the BN shown in Fig. 19, (Parhizkar et al., 2020b). The fault tree and BN are developed based on International Marine Contractors Association (IMCA) annual reports on station keeping incidents from 2004 to 2016 analysis (Parhizkar et al., 2020b). It should be noted that the parent nodes are connected to all human error types; however, for simplicity, this is not included in the figure.

3.7. Disconnection execution

After selecting the method of disconnection, the disconnection (DC) execution will be performed (sixth phase/column presented in Fig. 8). The probability of DC execution follows the same function as presented for the execution stage. In addition, the time allocated to DC execution consists of two main intervals.

One is the time allocated to activating the emergency disconnection by the operator/controller, which is an execution process, and its response time follows the same pattern as the execution stage. This time interval is denoted by "disconnection execution" in the results section.

The other time interval is the time it takes for the vessel to be disconnected and get back into a stable position. According to (Chen et al., 2008), it takes the vessel approximately 40 s to be disconnected and get back to a stable position. This time interval is denoted by "disconnection" in the results section.

3.8. End states

End states are the states at the end of the pathways (last phase/column presented in Fig. 8). They are classified into groups that can lead to successes or severity of consequences. In the case under study, three possible end states are considered as follow:

- OK: The drilling unit could maintain position and return to green region to operate normally.
- DC (disconnection): The drilling unit is disconnected appropriately.
- MD (mechanical damage): The drilling unit is not disconnected appropriately; and as a result, mechanical and/or environmental damages occur.

3.9. General solution algorithm

In the proposed model for the case study, Bayesian networks and fault trees, presented in Section 3, are solved and failure probabilities of each event is calculated; and finally based on Fig. 8 system end state

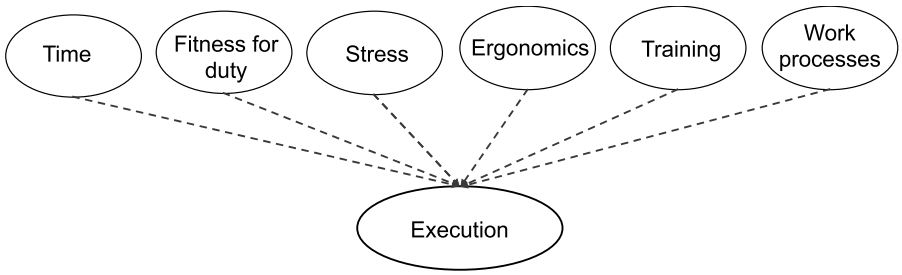


Fig. 15. Bayesian network of execution probability.

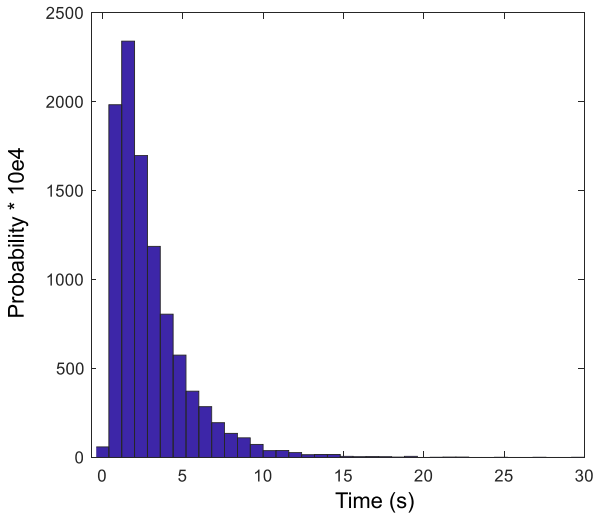


Fig. 16. RT distribution of the execution process.

probabilities are calculated.

The data flow starts with the Monte Carlo method. The time allocated to each event is a random value from a gamma/GIG distribution. In order to have a more realistic result, the Monte Carlo method is used and random times required for detection, diagnosis, decision making, and execution are selected from the generated distributions (Figs. 10, Figure 12, Fig. 14, and Fig. 16).

Time available is calculated based on the sensor data (ambient and operational conditions) using the dynamic simulator. In the dynamic simulator, the operational and environmental conditions of the DP system, including wave, current power system, control system and propulsion system characteristics, are taken as inputs. Using dynamic simulation, the position and the velocity of the DP system over time are calculated. The position and velocity of the DP system are used to calculate the time available before collision happens.

The required times (random numbers selected from distributions) and the time available are used to evaluate conditional probabilities using SPAR-H method (Table 1 and Eqs. (3)–(6)). The conditional probabilities, as well as sensor data and crew characteristics, enter Bayesian networks; and the failure probabilities of the human related events are quantified. The failure probabilities of technical events are evaluated using fault trees. Afterall, the end state probabilities of the ESD are calculated based on the derived probability of each event. This process is repeated for the predefined total number of Monte Carlo simulations. At each iteration, a random number from time allocated distributions will be selected and the process will be followed again, and end state probabilities will be calculated.

4. Results

4.1. Scope identification

In the case study, a DP drilling unit problem is provided to illustrate the methodology effectiveness. It is assumed that an initiating event has happened, and the system has entered the yellow region. Based on the system dynamic simulation results, the system will enter the red region after 500s. Therefore, the time available for decision-making and recovery action to get back to the position is 500s. On average, this is sufficient time to diagnose and take action. It is assumed that the disconnection would be performed automatically, if required.

It is assumed that the operator procedure and the human-machine interface have nominal effect on performance. According to (Whaley et al., 2011), the quality of the procedures is adequate, and they are assumed to be followed. Procedures do not reduce nor to a large degree increase performance. In addition, the human machine interface and physical working environment has neither a negative nor a positive effect on performance. All of the safety critical information is easily available, and no human machine interface-related issues are interfering with carrying out the task. In addition, crew characteristics are assumed as follow:

- Stress level: Operator(s) does not experience threat stress and the stress level has not a negative effect on performance.
- Training: The operator(s) has training on the task(s) in this scenario and has the necessary knowledge and experience to be prepared for and to do the task(s) in this scenario. The level of training does not reduce performance nor to a large degree improve performance.
- Fitness for duty: The operators have good attitudes to safety and work conduct and there is explicit management support to prioritize

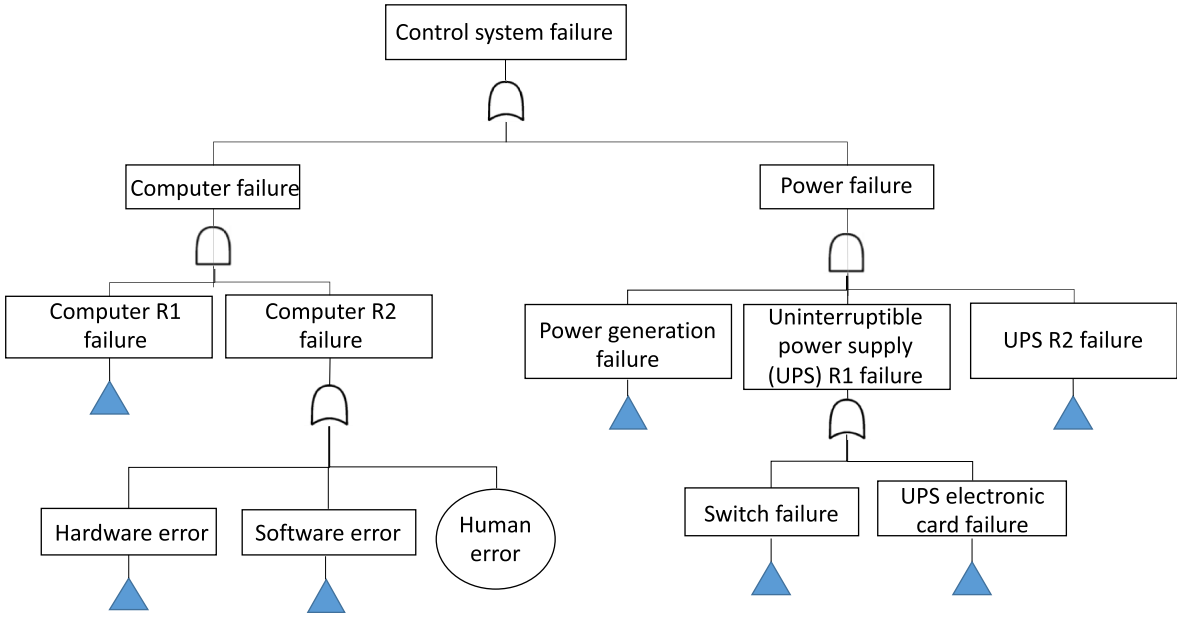


Fig. 17. Automatic disconnection fault tree of a DP drilling unit (Parhizkar et al., 2020b).

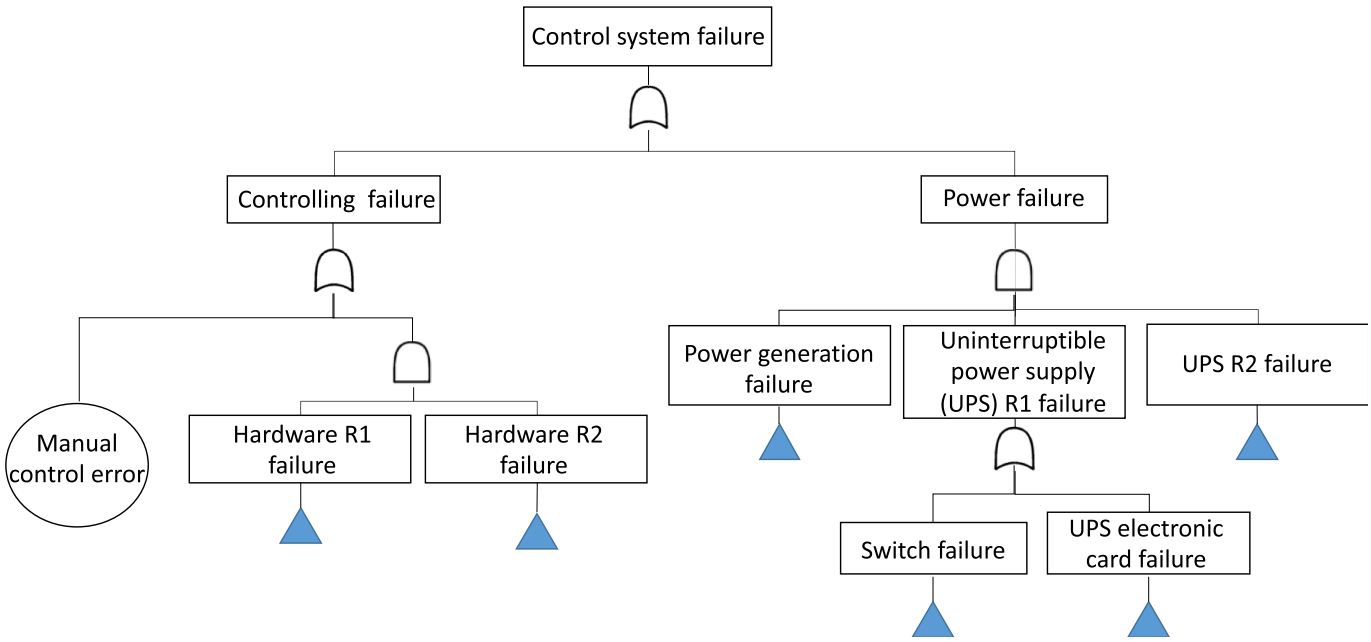


Fig. 18. Manual disconnection fault tree of a DP drilling unit (Parhizkar et al., 2020b).

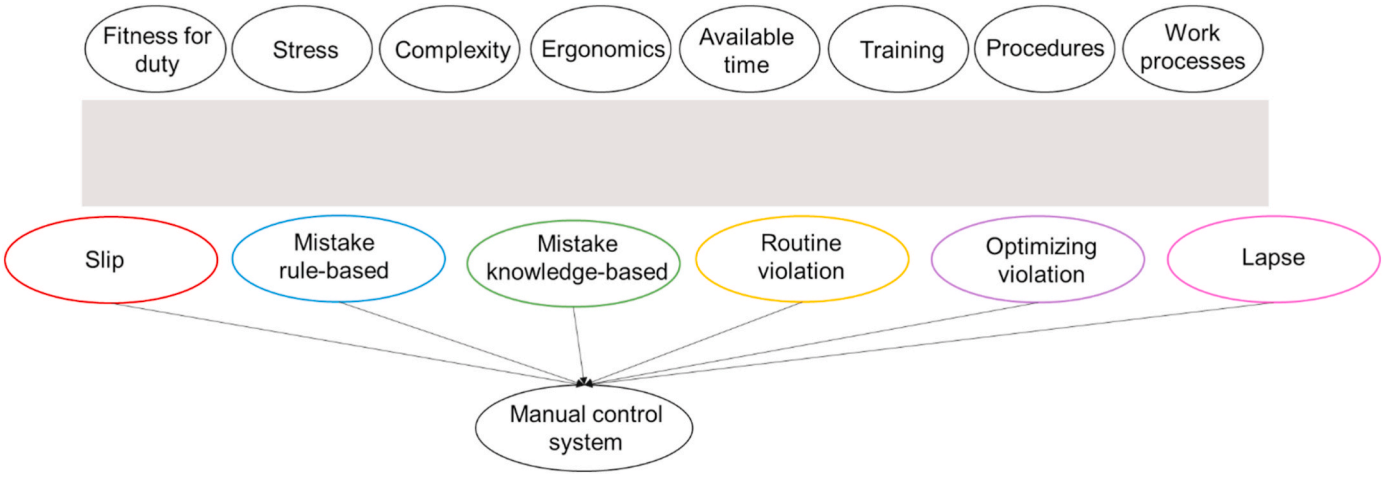


Fig. 19. Human error Bayesian network of manual disconnection (Parhizkar et al., 2020b).

safety when that is appropriate. The operator(s) also shows mindfulness about safety.

- Work processes: The teamwork is adequate on one or several teamwork factors that have been identified as important for the performance of the task or scenario in question. Teamwork has neither a negative nor a large positive effect on performance.

In addition, failure frequencies of basic events in fault trees are assumed equal to values presented in (Parhizkar et al., 2020b). These assumptions are taken as inputs to the flow diagram, illustrated in Fig. 20, and the probabilities of events as well as end states (Fig. 8) are calculated, which is presented in Section 4-2.

Moreover, sensitivity analyses on inputs are performed. In Section 4-3, incident scenarios with different available times (adequate time available, barely adequate time available, inadequate time available) are compared; and in Section 4-4, the results for incident scenarios with different complexity level are presented and compared.

4.2. Dynamic probabilistic risk assessment

Fig. 21 presents the probability distribution of all events in the decision-making process, including execution. The results are converged after selecting 10,000 random times allocated to each event. The values on the Y-axis are probability $\times$ 10e4, e.g., number 200 on Y-axis presents 200/10e4 = 0.02.

As can be seen, event probabilities are mostly between 0.8 and 1. As the time available before entering the red region is greater than the time required to make decision and execution, each event will have an adequate time to be performed. As a result, their accuracy (event probability) has a high level. In addition, as can be seen, the disconnection event has a constant probability of 0.9403 in all runs. The reason is that the disconnection process has a fixed time allocated, as mentioned in Section 3-7; therefore, the related fault tree and BN result in the same value for all 10,000 runs. However, in other events (detection, diagnosis, decision making, execution and disconnection execution), the probability of the event has a distribution. This is because the probability of these events are functions of the time allocated, which has

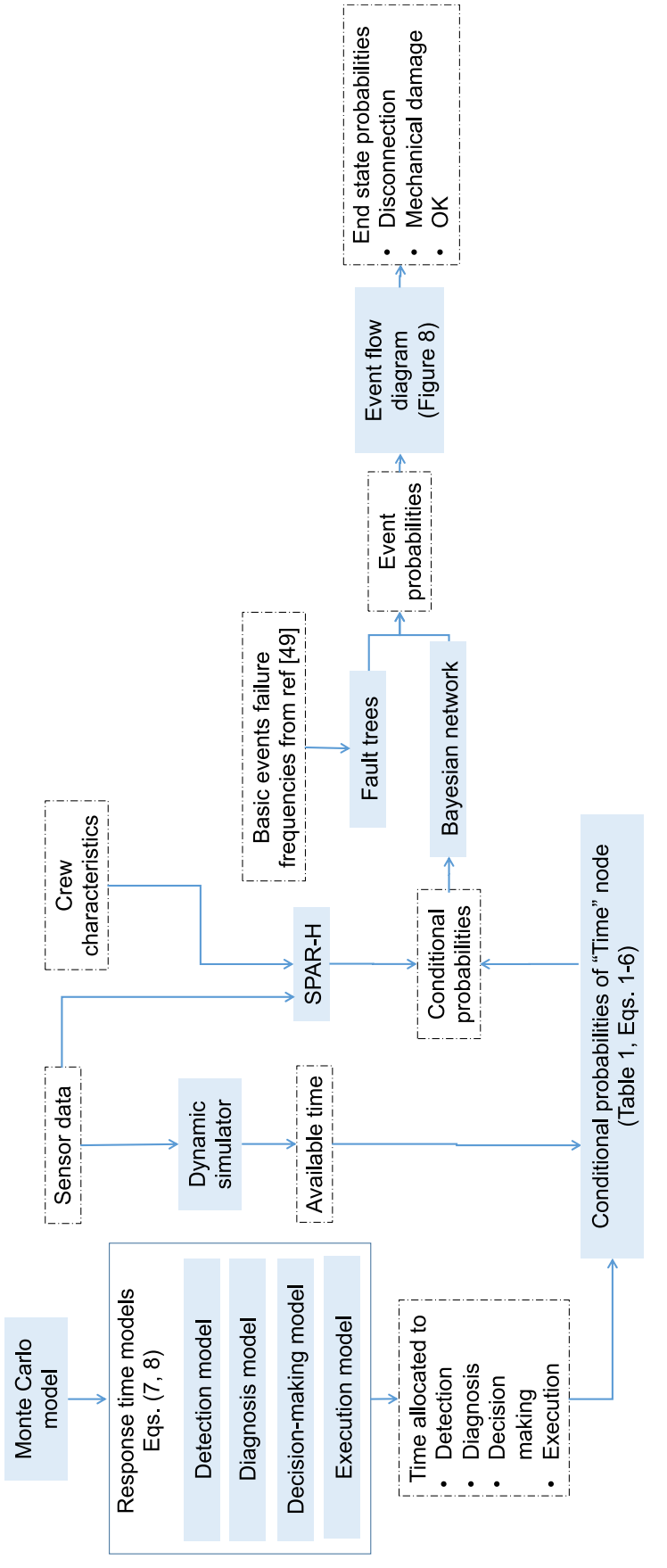


Fig. 20. Data flow diagram of the proposed methodology illustrated for the case study.

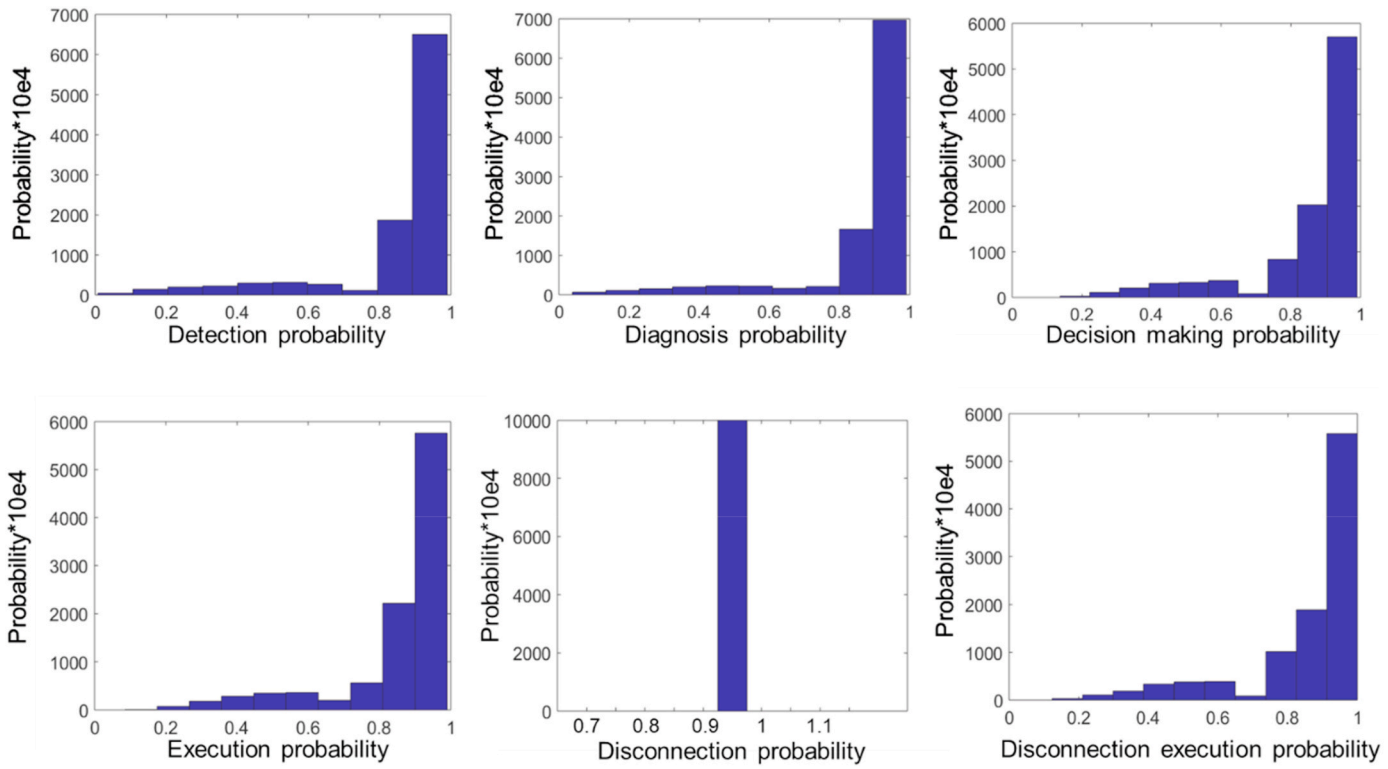


Fig. 21. Probability distribution of the decision-making process and action taking events (Detection probability: Section 3.1, Diagnosis probability: Section 3.2, Decision-making probability: Section 3.3, Execution probability: Section 3.4, Disconnection probability: Section 3.5, Disconnection execution probability: Section 3.7).

a probability distribution. At each run, a random number from the time allocated distribution is selected, and then the event probability is calculated accordingly. Thus, there are distributions for the mentioned events' probabilities, which are presented in Fig. 21.

As mentioned before, the end states of the scenario are OK, disconnection (DC), and mechanical damage (MD). Fig. 22 presents the occurrence probabilities and the mode values of these end states. The mode values present the most frequent result of the end states after running for 10,000 times. As is illustrated, the mode of the OK probability distribution is 0.951. It means that the probability of decision-making, action taking and get vessel back to a safe position, in less than 500s, is 0.951. Disconnection refers to an appropriate disconnection without any damage to the system, and its probability is 0.046. MD is a failure in proper disconnection. The mode probability of MD is 0.004 for the scenario under study.

Fig. 23 presents the time allocated distribution of all events in the decision-making and execution process. As can be seen, distributions follow almost the same pattern as the human RT distributions, as presented in Figs. 10, Figure 12, Fig. 14, and Fig. 16. The results are derived based on the 10,000 runs. As the number of runs increases, the pattern would be more similar to the presented human RT distributions.

According to (Byeet al., 2017), there are some overlaps between the performed tasks in the decision-making process steps. Considering the values presented in (Byeet al., 2017; Chen et al., 2008), the distribution of the overall time allocated from detecting an initiating event up to the end states is presented in Fig. 24. The mode of the distribution is 74.3 s. In other words, the decision-making process from detection to taking action takes about 74.3 s.

4.3. *Effect of time available on risk level*

After the detection of an initiating event, operator(s) should make a decision and take recovery actions before the vessel enters the red region. This forces a time constraint on the decision-making process. The

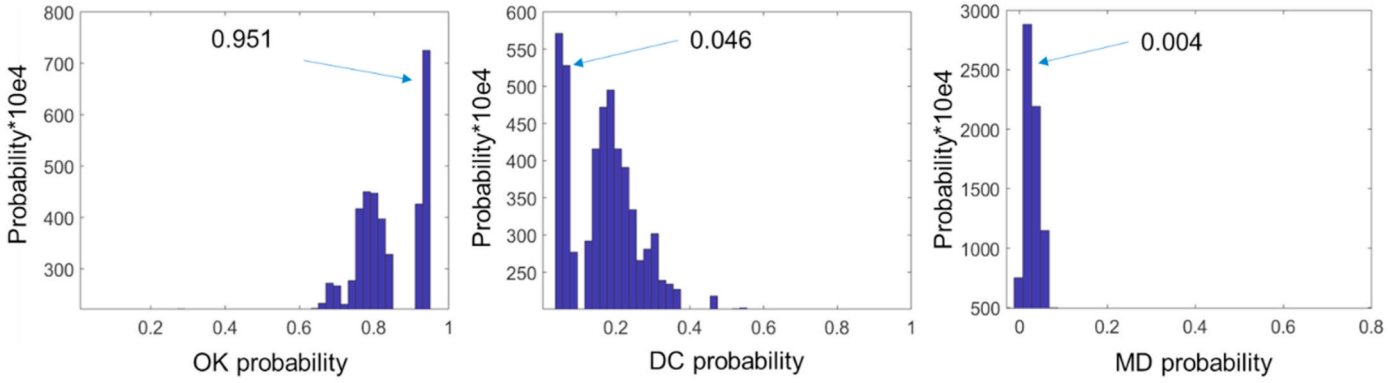


Fig. 22. End states probability distribution, (DC: disconnection, MD: mechanical damage).

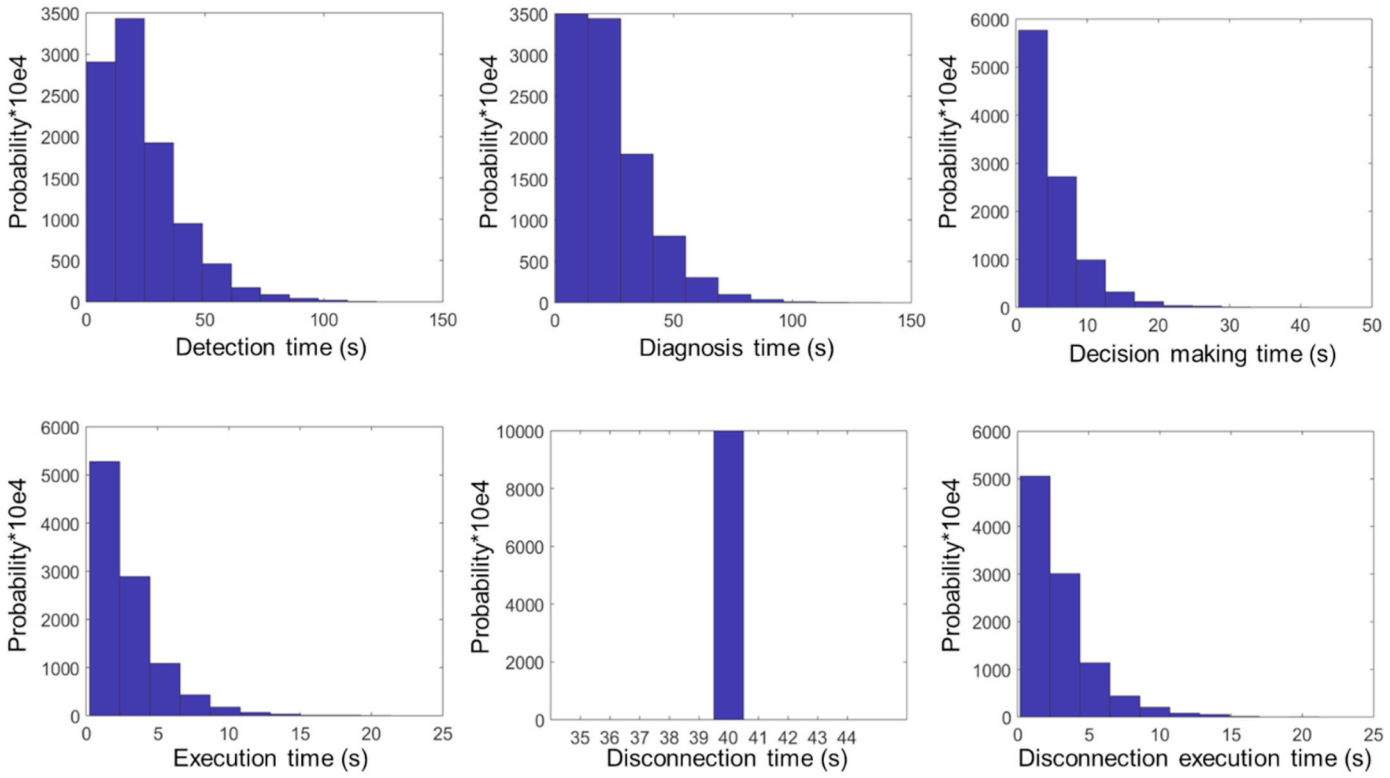


Fig. 23. Time allocated distribution for all decision-making and action taking process events (Detection probability: Section 3.1, Diagnosis probability: Section 3.2, Decision-making probability: Section 3.3, Execution probability: Section 3.4, Disconnection probability: Section 3.5, Disconnection execution probability: Section 3.7).

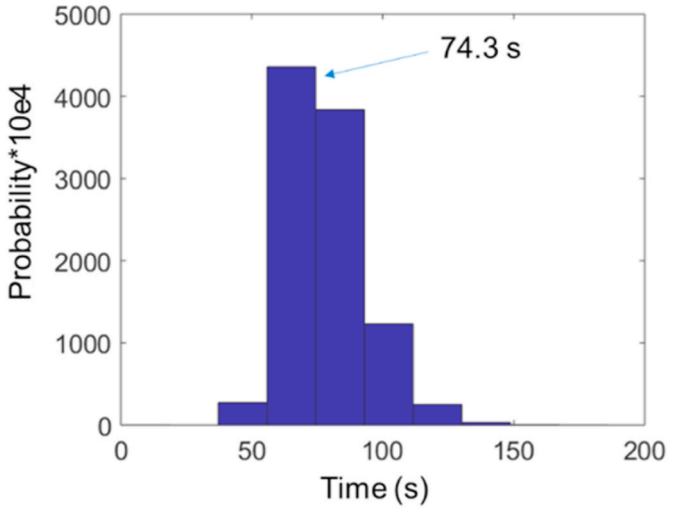


Fig. 24. Probability distribution of the overall time allocated from detection to taking action.

time constraint depends on the nature of the incident, vessel type, water deepness and other environmental factors. A dynamic simulator can be used to calculate this time constraint. After an initiating event, vessel position, incident details, and vessel characteristics are used as inputs to the simulator, and the simulator shows how long it will take for the vessel enters the red region. This time span is the time available to make a decision and perform a recovery action before entering the red region. In this section, the system risk level for three different scenarios, i.e., adequate time (500s), barely adequate time (200s), and inadequate time (100s) are compared. These timelines are inferred from (Byeet al., 2017; Marius et al., 2018).

Fig. 25 presents the probability of end states as a function of the time allocated for the scenario with adequate time available. In the graphs, each dot represents one run out of 10,000 times run of the model. It is shown that, as the time allocated increases, the probability of OK increases and reaches to 0.951 after about 150s – i.e., the probability of proper decision-making, action taking and get vessel back to the safe position, in 150s, is 0.951.

On the other hand, the probabilities of MD and DC decrease with increasing the allocated time. MD and DC end states approach 0.004 and 0.046, respectively. The approached value of DC is higher than MD due the adequate time available for the disconnection process. When there is sufficient time available, the disconnection could be performed appropriately, and its probability would be higher than MD.

Fig. 26 presents probability of end states as a function of time allocated for the "barely adequate time" scenario. In this scenario, it is assumed that the time available for decision-making and taking recovery actions and get vessel back to a stable position is 200s. As can be seen in the OK probability graph, some of the runs resulted in approximately 0 values (shown in red circle). These runs present scenarios in which operator(s)' decision-making or taking action has taken longer than time available (200s), and vessel is entered red region. In this scenario, due to the lack of time the probability of appropriate disconnection is low and, as a result it is highly probable that vessel loss its position.

Fig. 27 illustrates the probability of end states for a scenario with "inadequate time available". In this scenario, the time available for decision-making, action taking and get vessel back to a safe position is 100s. As can be seen in graphs, most of the runs take more than time available (100s). Consequently, the OK probability approaches 0.001 and MD approaches 0.998. As the time available is inadequate, there is no time to have an appropriate disconnection, and in most cases, the disconnection process results in mechanical damage.

Table 2 summarizes results of the three scenarios of adequate, barely

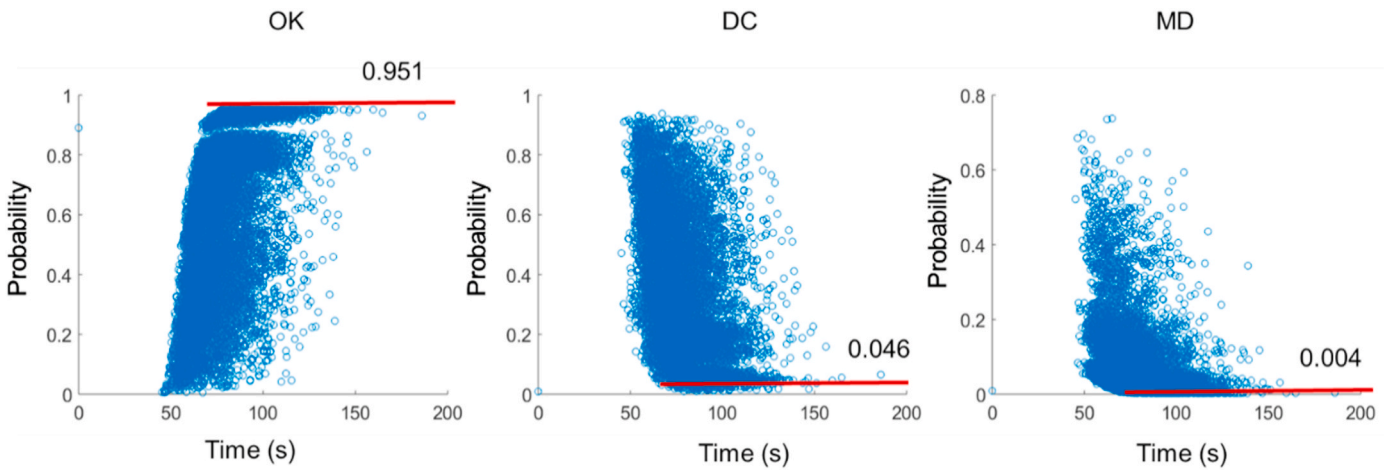


Fig. 25. Probability of end states for the "adequate time available" scenario, (DC: disconnection, MD: Mechanical damage).

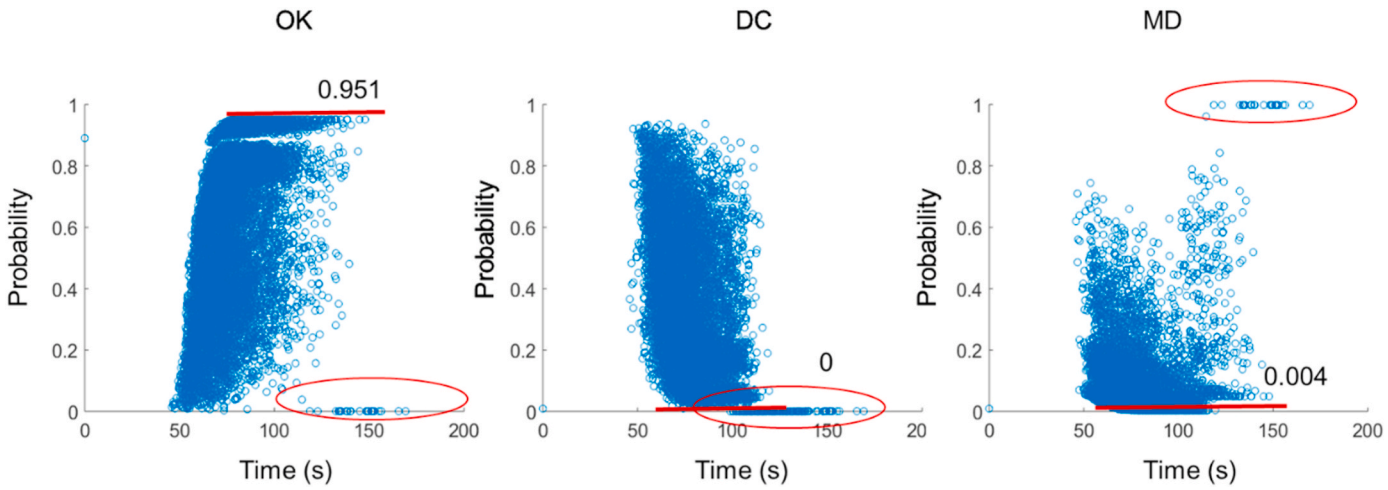


Fig. 26. Probability of end states for the "barely adequate time available" scenario (DC: disconnection, MD: Mechanical damage).

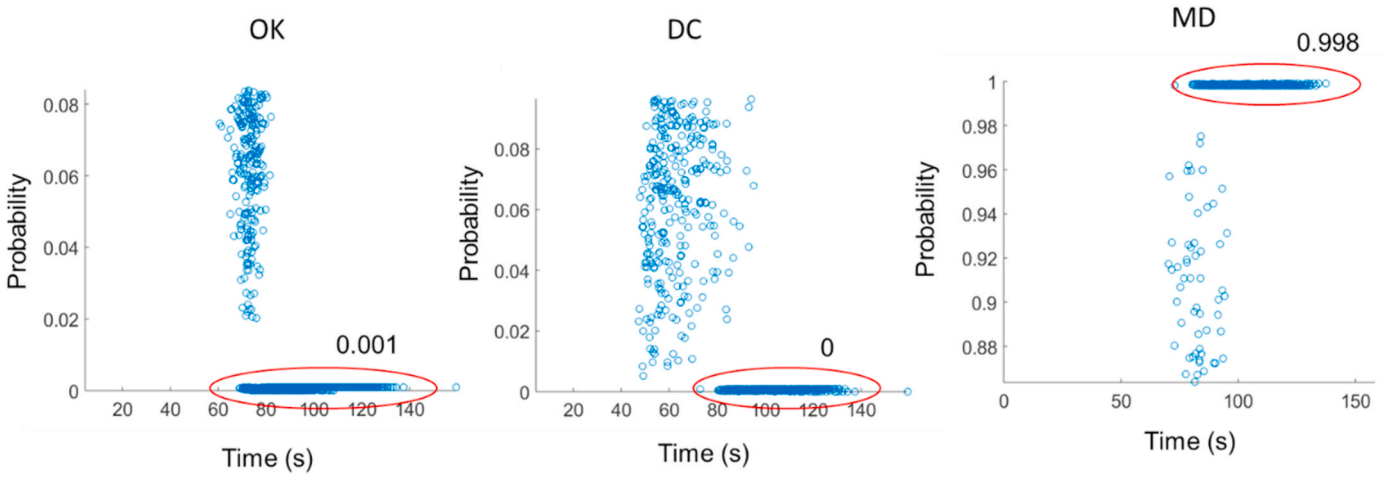


Fig. 27. Probability of end states for the "inadequate time available" scenario (DC: disconnection, MD: Mechanical damage).

adequate and inadequate time available. The presented values are the mode value of the probability distribution of each end state, as presented in Figs. 25–27. The mode value is the most frequent value presented in the distributions. Therefore, the sum of the probabilities presented in each column of Table 2 are not equal to one as they are not presenting a specific scenario's end state.

In addition, as can be seen, by decreasing the time available, the probability of appropriate disconnection is approaching to zero. The reason is that it is assumed that in all scenarios, the decision-making process follows the same pattern as presented in Fig. 8: Operator(s)

try to diagnose, make decision, execute, and if vessel enters red region; take disconnection action. Therefore, by decreasing the time available, there would not be sufficient time for end events such as disconnection. Moreover, in the "inadequate time available" scenario, there is a very low probability that the vessel gets back into its stable position and, the probability of MD is equal to 0.998.

4.4. Effect of incident complexity on risk level

The studied incident is not very complex and task complexity has neither a negative nor a positive effect on operator(s)' performance. In this section, a comparison between the studied incident (normal case) and a case with complex tasks (complex case) is performed. In the complex case, the tasks that should be performed are moderately complex. There is some ambiguity in what needs to be diagnosed or executed. Several variables are involved, perhaps with some concurrent diagnoses or actions (i.e., evolution performed periodically with many steps). In this situation, operator(s) performance is influenced negatively.

Fig. 28 presents the probability distribution of all events for both simple and complex cases. The blue graphs are the same as graphs presented in Fig. 21. In Fig. 28, most parts of the distributions have overlap. However, it can be inferred that the probabilities of all decision-making events, decrease in the complex case due to the negative influence of complexity on operator(s) performance. However, this effect is more significant in the diagnosis process. The reason is that complexity affects diagnosis performance dramatically, and this is shown in the related BN presented in Fig. 11. In addition, it is depicted that complexity has the least effect on the decision-making process, since at this step, making decisions based on the available diagnosed information would be performed and task complexity does not be affected the successful decision-making step considerably. This is depicted in the successful decision-making BN, presented in Fig. 13.

Fig. 29 presents the probability of end states for both the normal and complex cases. The OK probability decreases approximately to 0.186 (19 %) in the complex case. In addition, in the complex case, the OK probability increases more slightly as a function of the time allocated. However, in the normal case, the rate of increase is sharper. This shows that in the complex case, it takes more time to make an appropriate decision and take action. As a result, the rate of increase is not as sharp as in the normal case.

5. Discussion

5.1. The Dynamic nature of the study

The proposed framework aims to consider uncertain and time dependent risk influent factors and implement frequent updating of risk-related information during decision-making phases. The proposed event flow diagram concept combines the static analysis of BNs and fault trees with the dynamic analysis of event dependency and occurrence probability (Section 2). This combined analysis reveals that incident consequences are highly time dependent, and operator(s) can face an increased risk level as the time available for a specific incident decreases (Figs. 25–27).

More specifically, the proposed methodology considers time dependency in different parts of an analysis, including:

Table 2
Mode of probability distributions for three different scenarios.

End state/ Scenario	Inadequate time available	Barely adequate time available	Adequate time available
OK	≅ 0.001	≅ 0.951	≅0.951
DC	0	0	≅0.046
MD	≅ 0.998	≅ 0.004	≅0.004

1. The model updates the event connections using updates from sensor data and a dynamic simulator of the system. As a result, over time the event sequence diagram is updated.
2. The main difference between the proposed methodology and conventional methods is in the way that the model considers the failure probabilities as a function of required, available and allocated time to each event.

The conditional probability of the "Time" parent node in the Bayesian networks (Figs. 9, Figure 11, Figure 13, Figure 15) are dependent on the required, available and allocated time to each event (Eqs. (3)–(6)). The available time at each phase of the dynamic event sequence diagram (Fig. 8) is calculated based on the available time of incident minus time spent in the previous phases.

As the probability of an event depends on the available time; and the available time depends on the time spent on the previous events, we could say that the probability of an event depends on the allocated time to the previous events. That is one of the main novelties of this research that resulted in more realistic system failure probabilities in emergency situations.

3. In the proposed framework, all events have a time allocated (human response time). The human response time depends on the nature of the event and various environmental and physical factors that make the response time prediction complex. Many researchers have conducted studies on predicting the human response time, and there are many experimental data in this regard. In this study, the time allocated distributions for detection, diagnosis, decision-making and execution processes are estimated by using data-driven methods (Eqs. (7) and (8)).

5.2. The model applicability domain

In this paper, a dynamic probabilistic risk assessment method for the decision-making process in emergencies is proposed (Section 2). The proposed event flow diagram (Fig. 2) is applicable to different complex systems and application areas in an emergency. The model is able to predict dynamic probabilistic risk of decision scenarios over time. However, it should be noted that the related dynamic simulator of the system, BNs and fault trees should be adapted to each system accordingly. However, the concept and the steps that should be followed remains the same as the presented case study (Section 3).

5.3. Response time uncertainties

In the studied case, the process is simulated 10,000 times (Section 4-2). In each run, response times of detection, diagnosis, decision-making and execution are randomly selected from response time distribution models. Then, the probability of each event is calculated accordingly. The results of every run are collected, and a distribution of the results are presented in all graphs in the result section. Using this method, response time uncertainties in decision-making process is considered in the risk evaluation process.

5.4. Decision-support tool

The end states' probabilities as a function of time are presented for all runs (Figs. 25–27).

From the results, it can be seen that probability has an upper bound that could be reached in an adequate time span. This approached value as a function of time could assist decision-making process so that it could play a function for a similar situation. For example, the average required response time to reach maximum risk level could be derived for a different incident. This value is a critical information for operator(s) in emergencies to make an optimal decision such as recovery actions or shut down scenarios. Not only the average response time, but also the

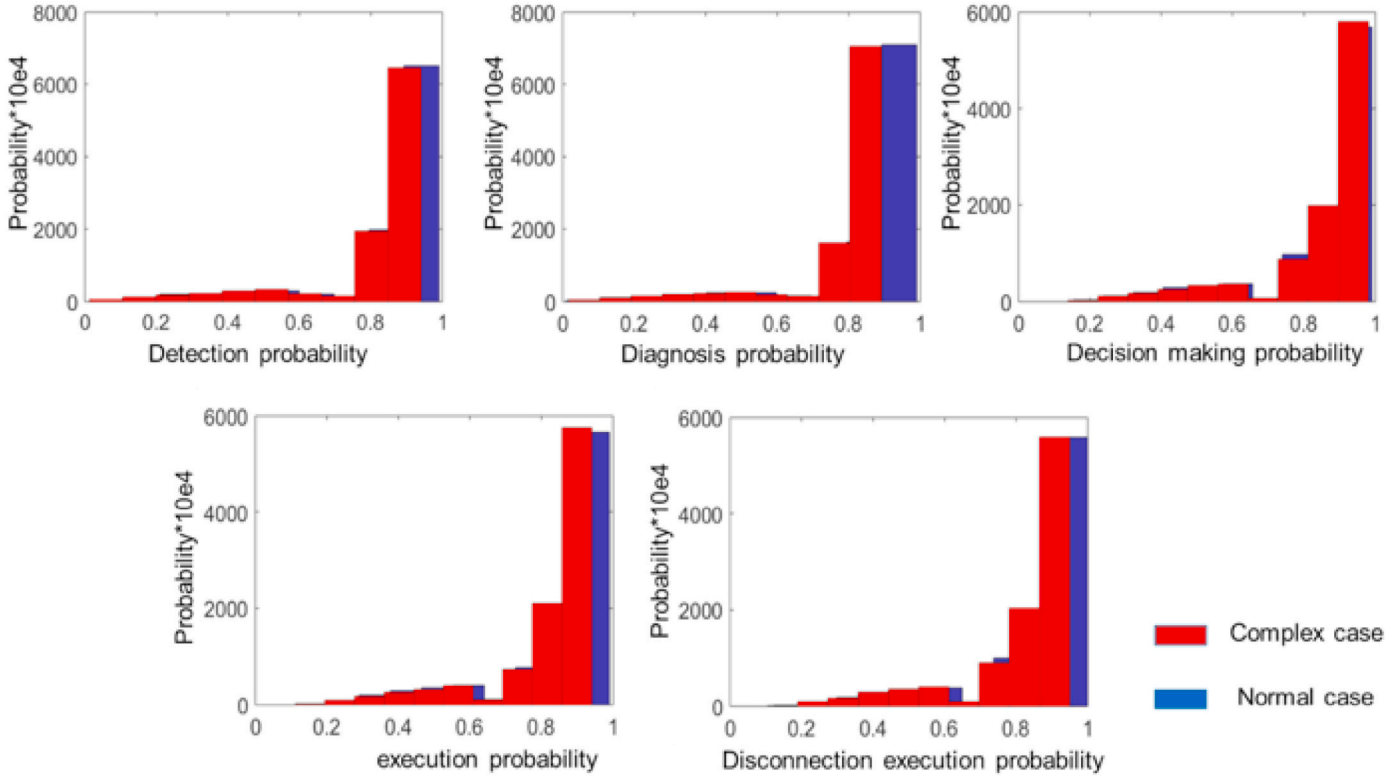


Fig. 28. Comparison between probability distribution of events in normal and complex cases (Detection probability: Section 3.1, Diagnosis probability: Section 3.2, Decision-making probability: Section 3.3, Execution probability: Section 3.4, Disconnection execution probability: Section 3.7).

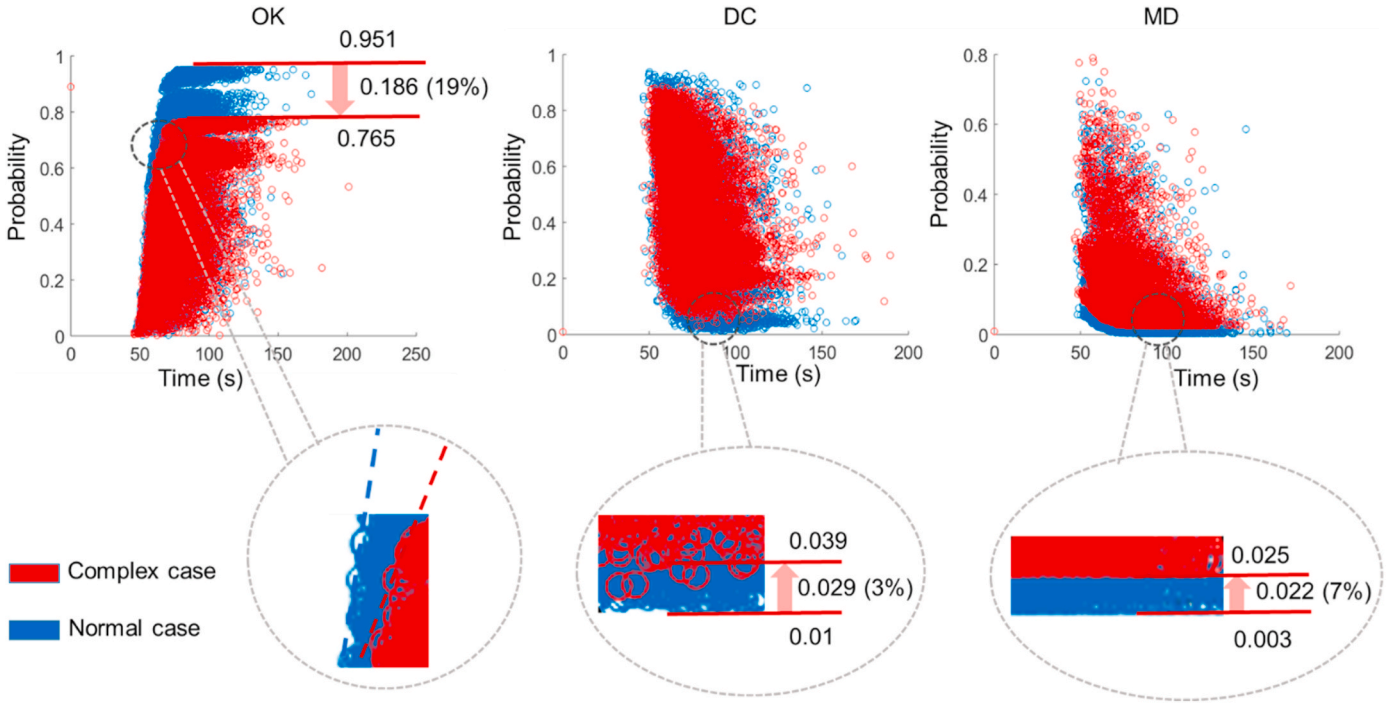


Fig. 29. Comparison between the probability distribution of the end states for normal and complex cases (DC: disconnection, MD: Mechanical damage).

maximum response time is an important metric for making decision those could be derived from the presented graphs. These are some examples of novel insights derived from the proposed model compared to the state-of-the-art risk assessment studies, as we have considered dynamic probabilistic dependencies.

In general, the results of the model (end state probabilities) could provide inputs to a decision support tool. A decision support tool assists operator(s) in making better and/or faster decisions. In a decision support tool, powerful predication capabilities are utilized that help operators improve the way they approach available information and assist

them to have a better understanding about system behavior. The proposed dynamic risk assessment model in this paper could provide information about failure probabilities as a function of time for multiple decision scenarios. This information can be used in decision support tools and improves their prediction capabilities significantly.

5.5. Future work

One of the main paths for future research is the potential in developing the current methodology from an analysis tool into an online decision support tool. Dynamic probabilistic risk assessment delivers a better risk picture and allow for making decisions according to the needs, going from a re-active emergency management to a pro-active approach where decision scenarios could be analyzed and anticipated based on real-time information. One possibility would be to simulate all alternative decision scenarios and provide an approximate time scale and risk level of each scenario. Another option would be to allow the operator(s) to be informed about the event and sequence probabilities in the near future. Knowing this information could help operator(s) to readjust system configuration with improved knowledge about the system.

6. Conclusion

In this study, a dynamic probabilistic risk assessment method for the decision-making process in emergencies is proposed. The framework is able to model the interactions between complex system operation and the decision-making process in a very short execution time. The predicted risk level is probabilistic and is updated over time by getting more information about system and human operations.

The complexity associated with system and human models and their interactions is considered by the event flow diagram concept, introduced in this study. In this concept, all events in a decision scenario have probabilities that are functions of the time allocated (response time). These functions are calculated based on the "nature" of the events. The concept considers system uncertainties using the Bayesian network method, and data-driven distributions. Finally, the Monte Carlo method is utilized to model stochastic behavior of the system and human responses.

A case study is performed on a dynamic positioning mobile offshore drilling unit, and results show that the proposed framework is able to evaluate the risk level of a decision scenario for an incident. A sensitivity analysis on the time available for decision-making and incident complexity are performed; and promising results have been reported not only with regards to risk assessment of decision scenarios but also with regards to the computational cost (less than 1 s per run). The interconnections between human and technical factors are modeled using the DPRA method; and more accurate risk levels of decision scenarios are achieved.

CRediT authorship contribution statement

Tarannom Parhizkar: Conceptualization, Methodology, Data curation, Formal analysis, Modeling, Validation, Writing – original draft. **Ingrid Bouwer Utne:** Methodology, Writing – review & editing, Supervision. **Jan Erik Vinnem:** Methodology, Writing – review & editing, Supervision. **Ali Mosleh:** Conceptualization, Methodology, Supervision.

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.

References

US Nuclear Regulatory Commission, 2006. Evaluation of Human Reliability Analysis Methods against Good Practices. NUREG-1842, Washington, DC.
Barua, S., Gao, X., Pasman, H., Mannan, M.S., 2020. J. Loss Prevent. Process Ind. Bayes. Netw. Based Dynam. Operat. Risk Assess. 41 (2016).
Batur, A., Schmidt, E.G., Schmidt, K.W., 2018. June). Computation of response time distributions for messages on the controller area network. In: 2018 IEEE 13th International Symposium on Industrial Embedded Systems (SIES). IEEE, pp. 1–10.
Bi, H., Si, H., 2012. Dynamic risk assessment of oil spill scenario for Three Gorges Reservoir in China based on numerical simulation, vol. 50, 1112–1118.
Boring, R., Gertman, D., 2016. P-203: Human Reliability Analysis (HRA) Training Course (No. INL/EXT-17-40997-Rev000). Idaho National Lab.(INL), Idaho Falls, ID (United States).
Bye, A., et al., 2017. The Petro-HRA Guideline.
Chang, Y.H.J., Mosleh, A., 2007a. "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents Part 1 : Overview of the IDAC Model, 92, 997–1013.
Chang, Y.H.J., Mosleh, A., 2007b. "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents . Part 2 : IDAC performance influencing factors model, 92, 1014–1040.
Chang, Y.H.J., Mosleh, A., 2007c. "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents Part 3 : IDAC operator response model, 92, 1041–1060.
Chang, Y.H.J., Mosleh, A., 2007d. "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents . Part 4 : IDAC causal model of operator problem-solving response, 92, 1061–1075.
Chang, Y.H.J., Mosleh, A., 2007e. "Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents Part 5 : dynamic probabilistic simulation of the IDAC model, 92, 1076–1101.
Chen, H., Moan, T., Verhoeven, H., 2008. Safety of dynamic positioning operations on mobile offshore drilling units. Reliab. Eng. Syst. Saf. 93 (7), 1072–1090.
Cojazzi, G., 1996. The DYLAM approach for the dynamic reliability analysis of systems. Reliab. Eng. Syst. Saf. 52 (3), 279–296.
Devooght, J., Smidts, C., 1996. Probabilistic dynamics as a tool for dynamic PSA. Reliab. Eng. Syst. Saf. 52 (3), 185–196.
Groth, K.M., Swiler, L.P., 2012. Use of a SPAR-H Bayesian Network for Predicting Human Error Probabilities with Missing Observations.
Hakobyan, A., Aldemir, T., Denning, R., Dunagan, S., Kunsman, D., Rutt, B., Catalyurek, U., 2008. Dynamic generation of accident progression event trees. Nucl. Eng. Des. 238 (12), 3457–3467.
Hockley, W.E., 1984. Analysis of response time distributions in the study of cognitive processes. J. Exp. Psychol. Learn. Mem. Cognit. 10 (4), 598.
Hogenboom, S., Parhizkar, T., Vinnem, J.E., 2021. Temporal Decision-Making Factors in Risk Analyses of Dynamic Positioning Operations, vol. 207. Reliability Engineering & System Safety, p. 107347.
Izquierdo, J.M., Labeau, P.E., 2004. The stimulus-driven theory of probabilistic dynamics as a framework for probabilistic safety assessment. In: Probabilistic Safety Assessment and Management. Springer, London, pp. 687–693.
Joe, J.C., Shirley, R.B., Mandelli, D., Boring, R.L., Smith, C.L., 2015. The development of dynamic human reliability analysis simulations for inclusion in risk informed safety margin characterization frameworks. Procedia Manuf. 3, 1305–1311.
Kanes, R., Clementina, M., Marengo, R., Abdel-moati, H., Crane, J., Luc, V., 2017. Journal of Loss Prevention in the Process Industries Developing a Framework for Dynamic Risk Assessment Using Bayesian Networks and Reliability Data, vol. 50, pp. 142–153.
Kloos, M., Peschke, J., 2006. MCDET: a probabilistic dynamics method combining M onte C arlo simulation with the discrete D ynamic E vent T ree approach. Nucl. Sci. Eng. 153 (2), 137–156.
Kolaczkowski, A., 2005a. Good Practices for Implementing Human Reliability Analysis (HRA). US Nuclear Regulatory Commission. Office of Nuclear Regulatory Research, Division of Risk Analysis and Applications.
Kolaczkowski, A., 2005b. Good Practices for Implementing Human Reliability Analysis (HRA). US Nuclear Regulatory Commission. Office of Nuclear Regulatory Research, Division of Risk Analysis and Applications.
Lewis, S.R., Cooper, S.E., Najafi, B., Collins, E., Hannaman, B., Kohlhepp, K., Julius, J., 2010. EPRI/NRC-RES Fire Human Reliability Analysis Guidelines. Sandia National Laboratories (United States). Funding Organisation. US Department of Energy.
Li, M., Liu, Z., Li, X., Liu, Y., 2019a. Dynamic Risk Assessment in Healthcare Based on Bayesian Approach, vol. 189, pp. 327–334. September 2018.
Li, X., Chen, G., Khan, F., Xu, C., 2019b. Dynamic Risk Assessment of Subsea Pipelines Leak Using Precursor Data, vol. 178, pp. 156–169. October 2018.
Marius, I., Kristin, F., Marianne, K., Salman, N., 2018. The Level of Automation in Emergency Quick Disconnect Decision Making.
Matsuoka, T., Kobayashi, M., 1988. GO-FLOW: a new reliability analysis methodology. Nucl. Sci. Eng. 98 (1), 64–78.
Meng, X., Chen, G., Zhu, G., Zhu, Y., 2019. Dynamic quantitative risk assessment of accidents induced by leakage on offshore platforms using DEMATEL-BN. In: ", vol. 11, pp. 22–32.
Murchison, N., Gilmore, W.E., 2018. Human Reliability Analysis (HRA): Comparison of Methods (No. SAND2018-5383PE). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
Norazahar, N., Smith, J., Khan, F., Veitch, B., 2018. The use of a virtual environment in managing risks associated with human responses in emergency situations on offshore installations, Vol. 147, pp. 621–628. October 2017.

Norazahar, N., Khan, F., Veitch, B., Mackinnon, S., 2018. Dynamic risk assessment of escape and evacuation on o ff shore installations in a harsh environment. In: “, vol. 79, pp. 1–6. February.
Palmer, E.M., Horowitz, T.S., Torralba, A., Wolfe, J.M., 2011. What are the shapes of response time distributions in visual search? J. Exp. Psychol. Hum. Percept. Perform. 37 (1), 58.
Parhizkar, T., Utne, I.B., Vinnem, J.E., Mosleh, A., 2020a. Supervised Probabilistic Risk Assessment of Complex Systems, Part 1. Reliability Engineering & System Safety, Submitted.
Parhizkar, T., Hogenboom, S., Vinnem, J.E., Utne, I.B., 2020b. Data Driven Approach to Risk Management and Decision Support for Dynamic Positioning Systems, vol. 201. Reliability Engineering & System Safety, p. 106964.
Parhizkar T., Mosleh A., Supervised Probabilistic Risk Assessment of Complex Systems, Part 2: Application to Risk-Informed Decision Making, Practice and Results, Reliability Engineering & System Saftey, Submitted.".
Røed, W., Mosleh, A., Vinnem, J.E., Aven, T., 2009. On the use of the hybrid causal logic method in offshore risk analysis. Reliab. Eng. Syst. Saf. 94 (2), 445–455 (Chicago).
Swain, A.D., Guttmann, H.E., 1983. Handbook of Human-Reliability Analysis with Emphasis on Nuclear Power Plant Applications. Final Report (No. NUREG/CR–1278). Sandia National Labs.
Tombuyses, B., Labeau, P.E., Marchand, S.S., 1998. DDET and Monte Carlo simulation to solve some dynamic reliability problems. In: Proceedings of PSAM4, pp. 2055–2060.
Utne, I., Hokstad, P., Vatn, J., 2011. A method for risk modeling of interdependencies in critical infrastructures. Reliab. Eng. Syst. Saf. 96 (6), 671–678.
Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016. “Towards dynamic risk analysis : a review of the risk assessment approach and its limitations in the chemical process industry. Saf. Sci. 89, 77–93.
Vorobyev, Y., Kudinov, P., 2011. March). Development and application of a genetic algorithm based dynamic pra methodology to plant vulnerability search. In: International Topical Meeting on Probabilistic Safety Assessment and Analysis, vol. 1, pp. 559–573.
Wang, C., 2007. Hybrid Causal Logic Methodology for Risk Assessment (Doctoral Dissertation).
Wang, H., Khan, F., Ahmed, S., Imtiaz, S., 2016. Dynamic quantitative operational risk assessment of chemical processes. In: “, vol. 142, pp. 62–78.
Whaley, A.M., Kelly, D.L., Boring, R.L., Galyean, W.J., 2011. SPAR-H Step-by-step Guidance.
Wreathall, J., Roth, E.M., Bley, D., Multer, J., 2003. Human Reliability Analysis in Support of Risk Assessment for Positive Train Control (No. DOT-VNTSC-FRA-03-03). Federal Railroad Administration, United States.
Yau, M., Guarro, S., 1996, June. Dynamic flowgraph methodology (DFM) for safety analysis of critical control software. In: 3rd International Conference on Probabilistic Safety Assessment and Management (PSAM-3).
Zandt, T.V., 2002. Analysis of Response Time Distributions. Stevens’ Handbook of Experimental Psychology.
Zhang, N., Ni, X.Y., Huang, H., Duarte, M., 2017. “Risk-based personal emergency response plan under hazardous gas leakage : optimal information dissemination and regional evacuation in metropolises, 473, 237–250.
Zhang, L., Wu, S., Zheng, W., Fan, J., 2018. A dynamic and quantitative risk assessment method with uncertainties for o ff shore managed pressure drilling phases, 104 (January), 39–54.
Ma, T., Holden, J.G., Serota, R.A., 2016. Distribution of human response times. Complexity 21 (6), 61–69.