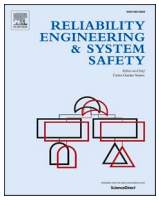
Reliability Engineering and System Safety 248 (2024) 110152

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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



A method for safety analysis of human-machine systems based on dynamic Bayesian simulation

Xing Pan *, Hengte Du, Haofan Yu

School of Reliability & Systems Engineering, Beihang University, Beijing, China

ARTICLE INFO

Keywords:
Human-machine systems
Dynamic bayesian networks
Gibbs Sampling
Safety Analysis

ABSTRACT

Accidents in human-machine systems often lead to serious consequences, so safety analysis is very important for such systems. However, the existing approach to safety analysis of human-machine systems lacks clear delineation of the coupling relationships between human and machine, or provide quantitative analysis. To address these issues, this paper proposes a method for safety analysis of human-machine systems, utilizing dynamic Bayesian network (DBN) and dynamic fault tree (DFT). The core of this method is the identification of human-machine coupling relationships, proposing 10 types of logical relationships and presenting corresponding DFT logic. Then, a conversion method from DFT to DBN is designed to avoid combinatorial explosion in complex FTA calculations. Based on the DBN model, simulation is conducted using Gibbs sampling, which offers higher computational efficiency. Additionally, a method for importance analysis is devised to identify critical nodes that impact the system risk. At last, a case study of refueling mission at space launch site is given to illustrate how to apply the method. Through simulation analysis, the safety risks during the refueling mission are quantitatively assessed, while critical nodes are identified. The results indicate that the dynamic Bayesian simulation method is good in information utilization, dynamic representation, and time performance.

1. Introduction

With the development of science and technology, human-machine systems have performed better with increasingly complex structures [1]. Composed primarily of complex machines, such systems involve a lot of work for operators, who, according to statistics, are related to 20–90 % of system failures [2]. The resulting safety accidents may cause great harm to both the people and the equipment [3,4]. Therefore, to assess system safety, it is not enough to just analyze the safety of the machine; safety analysis from the level of human-machine systems is necessary. As a typical dynamic system, human-machine systems can be analyzed for safety using dynamic reliability methods [5]. However, it differs from purely hardware-based dynamic systems. When analyzing its safety, it is also necessary to analyze the interaction between human and machine operations. Considering these factors, the current methods for safety analysis of human-machine systems face three main challenges. Firstly, the dynamic of human-machine systems can impact safety assessment by causing changes in structure, logic, and parameters, thereby altering the faults of the systems, necessitating more accurate model representations [6]. Secondly, the complex coupling relationship between humans and machines, which leads to safety failures, requires clarification of its logic before quantitative analysis [7]. Thirdly, for many existing methods such as the dynamic Bayesian network (DBN), directly modeling the structure of complex human-machine systems and obtaining conditional probabilities often entails a significant workload [8].

In the field of system safety assessment, probabilistic safety assessment (PSA) is one of the most popular methods. PSA usually adopts logical graph method, flow chart method, and state transfer method to complete the assessment [9,10]. Based on the state of the system, PSA includes static methods and dynamic methods [11]. The static methods of PSA include fault tree analysis (FTA), Bayesian network (BN) and so on, while the dynamic methods include event sequence diagram, GO-FLOW method, Markov-state-transition method, Petri net method, etc. In the static situation, FTA and BN are representative methods. FTA has a clear description of fault logic [12], which enables the quantitative calculation of system failure (or top event) probability [13]. BN can simplify calculations and quantitatively evaluate the safety of human-machine systems with the support of relevant algorithms and software tools [14]. With the development of simulation technology in

* Corresponding author.
E-mail address: panxing@buaa.edu.cn (X. Pan).

https://doi.org/10.1016/j.ress.2024.110152
Received 25 July 2023; Received in revised form 3 March 2024; Accepted 20 April 2024
Available online 21 April 2024

recent years, BN has a broader application in human-machine systems [15]. However, in practice, the operation tasks tend to continue over time [16], and the human-machine systems have very obvious dynamic characteristics, which is fundamentally different from the case in static methods.

Researchers have introduced DBN and dynamic fault tree (DFT) to meet the demands of dynamic system analysis [17,18]. DBN can describe the dynamic changes of human-machine systems well and enable quick quantitative analysis. On the basis of DBN, researchers designed the DBN simulation method. This DBN reasoning method based on simulation can greatly shorten the calculation time and improve the reasoning efficiency, which has become the focus of DBN reasoning algorithm research [19]. But for complex systems, it is difficult to directly obtain the structure and conditional probability of DBN. Unlike DBN, DFT can easily describe and display the fault logic in dynamic human-machine systems. However, since DFT is based on Markov model, a combinatorial explosion will occur if DFT is used for the analysis of large, complex, multimodal or multiphasic systems. [20]. As the number of cut sets increases exponentially with system size, it becomes difficult to calculate the probability of top events for complex systems [21]. A better solution to dynamic human-machine system analysis is found in this paper by combining DBN with DFT: identify the fault logic to get DFT, then convert DFT into DBN, and finally use DBN for calculation. The difficulty in this method is to identify the fault logic of human-machine systems.

In human-machine system research, fault logic identification methods can mainly be divided into two categories. Those in the first category separate people from machines and study each other independently. Such methods generally focus more on either human or machine [22]. For example, [23] emphasized human failure and regarded human beings as the main contributors to system failures. In addition, some studies have also analyzed both human and machine and superimposed one on the other to obtain conclusions [24,25]. Although this method is convenient for model construction and solution, it does not consider the deep mechanism of human-machine interaction. Methods in the second category take human as a part of the system environment for human-machine feedback research. In such studies, human factors can interact with machines in both directions [26] or one of them [27], thus influencing machine failures [28]. However, these studies only take into account the impact of machine failures on the system, but not the impact of human errors. To reflect the impact of human errors, a more complex human-machine-environment system can be constructed, and human errors can be used as environmental feedback for reliability analysis [29], but this will result in a larger amount of calculation [30]. The second kind of methods can reflect the human-machine interaction to some extent, but they do not analyze machine and human as two main parts of the system, and there is a lack of relevant concepts to describe the coupling logic between human errors and machine failures. In summary, there is a limited amount of literature available for studying the coupling mechanism between humans and machines, as both are considered equal in the system. Consequently, there is a scarcity of direct theoretical references for describing the failure mechanism of human-machine systems.

To solve the problems discussed above, this paper provides a safety analysis method based on dynamic Bayesian simulation. It first divides the faults in a human-machine system into human errors and machine failures and studies the coupling relationship between them. Based on the logic between human errors and machine failures, it constructs the DFT model of the human-machine system. Then, the DFT is transformed into DBN using specific conversion methods. In this way, it not only gives full play to the advantages of DBN in quantitative analysis, but also solves the problems of building complex BN and the combinatorial explosion caused by directly solving the DFT. After obtaining the DBN, the Gibbs sampling method is used for simulation to avoid the long solution time for complex system network. In order to evaluate the simulation results, an importance analysis of each node is designed to facilitate weak point identification. Finally, a case study of aerospace fuel filling is conducted to verify the effectiveness and advantages of this method.

The paper is organized as follows. Section 2 proposes the basic framework of the dynamic Bayesian simulation method. Section 3 presents the process of dynamic Bayesian simulation method. In Section 4, the method is applied to an aerospace fuel filling process to show its effectiveness and advantages. Conclusion is reached in Section 5.

2. Framework

As Fig. 1 shows, the dynamic Bayesian simulation method for safety analysis of dynamic human-machine system is divided into three stages: system analysis, system modeling and system assessment. A loop interface for feedback and inspection is also included in this method.

Stage 1: System Analysis

Before the safety analysis, the human-machine system needs to be analyzed first. In the preliminary analysis, it is necessary to clarify the content of the system boundary, system composition, and operation mechanism. Then the data of the human errors and machines failures in the system is collected. Sufficient data can bring more accurate analysis results.

Based on the collected data, the fault logic in the system is identified through two steps. Firstly, draw the man-in-the-loop control diagram of each system fault. Secondly, list all human errors and machine failures in the system and compare them with the human-machine system fault logic table (Table 1) to match their fault logic. In this paper, 10 kinds of human-machine fault logic are summarized. They can not only fully explain the fault mechanism of human-machine systems, but also represent the vast majority of the fault modes in human-machine systems.

Stage 2: System Modeling

After determining the logic corresponding to the nodes, the DFT is established based on logic gates. Then the logic gates in the DFT are converted into DBN fragments. Finally, these DBN fragments are integrated into a complete DBN. Steps in this stage can be carried out according to the method provided in Section 3. These steps usually remain unchanged for different human-machine systems.

Stage 3: System Assessment

System assessment begins with obtaining the DBN. The reasoning algorithms of DBN mainly include exact reasoning algorithms and approximate reasoning algorithms. For complex systems such as human-machine systems, exact reasoning algorithms are too slow and have a lot of other limitations. Therefore, approximate reasoning algorithms are more often used. As an approximate reasoning algorithm, simulation has become one of the most widely used reasoning algorithms due to its short calculation time and high reasoning efficiency [31], and Gibbs sampling is a good choice for quick and accurate system safety analysis. Therefore, this paper uses the extended Gibbs sampling method to specify the length of the Markov chain and the number of time slices, thus obtaining the required posterior distribution samples.

Using the data obtained from the simulation, the importance analysis can be carried out. Based on the perspective of system safety concerns, a series of indicators need to be designed to complete the importance analysis. Analyze the weakest node or nodes in the current system, and take targeted measures to improve it. Input the improved human-machine system into stage 1, and re-execute the dynamic Bayesian simulation until the system safety meets the requirements.

Compared with previous methods of human-machine system safety evaluation, the dynamic Bayesian simulation method can better reflect the human-machine coupling relationship and provide continuous optimization and feedback, thus enabling improvement of the system for a long time. Specific steps of the method will be introduced in the next section.

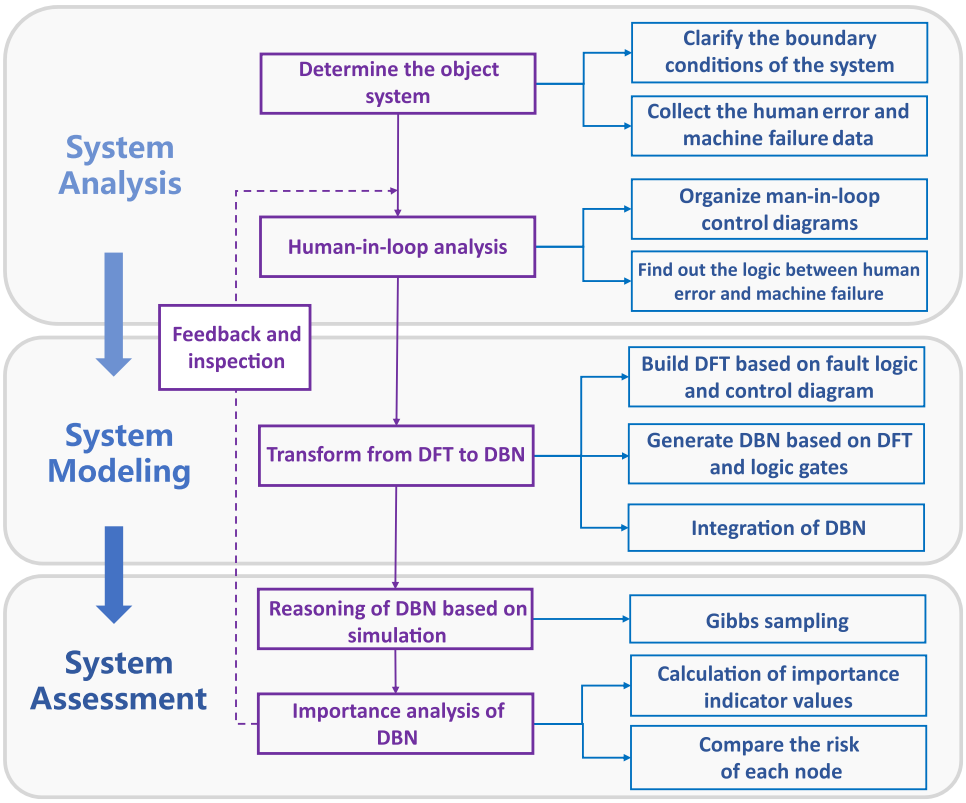


Fig. 1. The dynamic Bayesian simulation method.

3. Dynamic bayesian simulation method

3.1. Obtain the fault logic to build the DFT

In human-machine systems, a significant number of human operational errors and machine failures exist, which ultimately lead to accidents. The DFT is an effective method for describing the fault logic of such dynamic human-machine systems. DFT mainly utilizes events, logic gates, and other symbols to describe the time-varying causal logic relationship between fault events of dynamic system. Compared with the static FT, the most significant feature of DFT is its utilization of dynamic logic gates. Dynamic logic gates mainly include priority-AND (PAND) gates, sequence-enforcing (SEQ) gates, spare (SP) gates, and functional-dependency (FDEP) gates. With these dynamic logic gates, complex dynamic human-machine systems can be easily modeled.

To establish a DFT of human-machine system, the first thing is to identify the top event for the DFT, which typically represents a system failure that could lead to a serious accident. Then, it is necessary to clarify the boundary conditions of the system, as well as to identify the human nodes and the machine nodes. Next, the fault logic in the human-machine system needs to be determined, so as to complete the modeling of the DFT's structure.

Fig. 2 is an example of DFT in a human-machine system. *Y* indicates a system fault. From *A* to *E*, the white nodes represent machine failures and the nodes of the slash line represent human errors. The five nodes constitute a SEQ gate and a static gate respectively. These two logic gates affect system failures through another static gate. The probability calculations of these logic gates will be specifically introduced in Section 3.2.

However, the core feature of human-machine systems is the existence of a large number of human-machine interactions, which makes it difficult to obtain the DFT directly. Compared to other dynamic systems, human-machine systems exhibit more complex coupling relationships between humans and machines, posing a significant challenge for safety analysis. This complexity constitutes one of the core issues addressed in this paper, making the analysis of fault logic as a critical aspect in establishing DFT. To draw the DFT, it is necessary to sort out the fault logic of human-machine systems according to the characteristics of people and the system.

To delineate the fault logic, it is necessary to start from the root causes of failures in human-machine systems. Given the multitude of interactions and complex control relationships inherent in such systems, an initial analysis of the control relationships is paramount. In modern human-machine systems, which feature a high degree of automation, people mostly play the role of a monitor, and in a few cases, they play the role of a manipulator. As monitors, people obtain the information fed back by the monitoring machine and perform the next operation according to the regulations or personal judgment. After the operation is completed, the state of the monitoring machine is updated to generate new information, according to which people adjust their behaviors. This process is essentially a human-in-the-loop control process. A simple human-in-the-loop control diagram is shown in Fig. 3.

The human-in-the-loop control diagram shows the logic between human errors and machine failures. Since the occurrence of human-machine system failures is often hierarchical, the human-machine coupling relationship reflected in the man-in-the-loop control diagram can be divided into two types: same-level coupling and cross-level coupling. This classification stems from the causal relationship between human errors and machine failures in the faults. The same-level coupling means that two different types of fault events are the cause of logic gates, and the cross-level coupling means that one type is the cause of logic gates and the other is the result. Since the occurrence of faults in human-machine systems is often time-dependent, the logical relationship between human errors and machine failures can also be divided into time-dependent logic and time-independent logic. Time-dependent refers to the occurrence of system failures only when human errors and machine failures happen in a specific sequence [32]. Not all logic has time-dependent variations, Fig. 4 summarizes various

Table 1
(a). Time-independent logic in human-machine systems.

Coupling relationship	Type	Description
Same-level coupling	Same-level AND logic	At a certain level, both human errors and machine failures exist, and both of them occur, leading to subsequent higher-level human errors or machine failures.
	Same-level OR logic	At a certain level, both human errors and machine failures exist. If either of them occurs, subsequent higher-level human errors or machine failures will occur.
Cross-level coupling	Cross-level AND logic	At a certain level, only human errors exist, and all human errors occur, leading to subsequent higher-level machine failures. At a certain level, only machine failures exist, and all machine failures occur, leading to subsequent higher-level human errors.
	Cross-level OR logic	At a certain level, only human errors exist, and as long as one human error occurs, subsequent higher-level machine failures will occur. At a certain level, only machine failures exist, and as long as one machine failure occurs, subsequent higher-level human errors will occur.

Table 1(b). Time-dependent logic in human-machine systems

Coupling relationship	Type	Description
Same-level coupling	Same-level PAND logic	At a certain level, human errors occur first, and then machine failures occur (or machine failures occur first, and then human errors occur), leading to higher-level human errors or machine failures.
	Same-level SEQ logic	At a certain level, both human errors and machine failures exist, and multiple human errors and machine failures occur in a certain order, leading to higher-level human errors or machine failures.
	Same-level SP logic	At a certain level, human errors occur first, and then spare parts begin to work and fail, leading to higher-level human errors or machine failures. At a certain level, machine failures occur first, and human errors occur when operating spare parts, leading to higher-level human errors or machine failures.
	Same-level FDEP logic	At a certain level, a certain human error or machine failure occurs, causing a human error or machine failure related to the previous one's function.
Cross-level coupling	Cross-level SEQ logic	At a certain level, only human errors exist and they occur in a certain order, leading to subsequent higher-level machine failures. At a certain level, only machine failures exist and they occur in a certain order, leading to subsequent higher-level human errors.
	Cross-level SP logic	At a certain level, machine failures occur first, and then spare parts begin to work and fail, leading to subsequent higher-level human errors.

types of logic under the two classifications. Specifically, Table 1(a) introduces types of time-independent logic and Table 1(b) presents types of time-dependent logic.

It is worth noting that the cross-level PAND logic and the cross-level FDEP logic are not given in the cross-level time-dependent logic. This is because the cross-level PAND logic is rare in actual human-machine systems and can be replaced by the cross-level SEQ logic, and the FDEP logic generally only exists at the same level. In addition, in actual human-machine systems, the judgment of the same-level coupling and that of the cross-level coupling are not parallel but sequential, with the latter preceding the former. Based on the logic between human errors and machine failures, the logic gates in the system can be determined according to their corresponding relationships (Table 2).

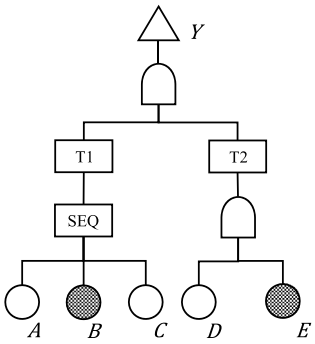


Fig. 2. An example of DFT in a human-machine system.

The various types of fault logic summarized above facilitate the modeling of human-machine systems using DFT. However, the state space of DFT increases exponentially with the increase of system size, and direct solution usually causes state space explosion for complex human-machine systems. A more convenient way is to use DBN that utilizes historical data for quantitative calculation. The subsequent step is to transform from DFT to DBN of human-machine systems.

3.2. Generate DBN based on DFT

DBN is a probabilistic network based on static BN and hidden Markov model [33]. Compared with static BN, DBN consider the changes of state variables over time, while also encompassing both causal logic and temporal logic. Generally, it is composed of two parts: the initial network and the transfer network [34]. It can be regarded as a set of static BNs, each of which is corresponding to a time slice whose structure remains the same as that of the previous or next time slice.

Supposing that the number of time slices in a human-machine system is T and $T > 1$, each time slice can be represented as $G_T = <<< H,M>_T, E_T>,P >$. $(H,M)_T$ is the set of all nodes in the time slice T. In addition, H_T and M_T represent the set of human error nodes and the set of machine failure nodes in the time slice T respectively. E_T is the set of intra slice arcs and inter slice arcs in the time slice T. Supposing the set of human error nodes is $H_T = \{H_T^1, ..., H_T^n\}$, $H_T^1, ..., H_T^n$ represents the states of n different human error nodes at T respectively. Similarly, $M_T^1, ..., M_T^n$ represents the states of n different machine failure nodes at T respectively.

Fig. 5 shows a simplified version of DBN. In this network, only the initial network in the time slice T and the transfer network from T to $T + \Delta T$ are drawn, and the rest of the nodes at T are omitted because the topological structure is completely consistent with that at $T + \Delta T$.

The adjacent time slices of DBNs are connected by directed arcs. These directed arcs are called the transfer network, which is essentially a set of conditional probability distributions (CPDs). These CPDs can be expressed as:

$$P\left((H,M)_{T+\Delta T}\middle|(H,M)_T\right) = \prod_{i=1}^{n} P\left((H,M)_{T+\Delta T}^{i}\middle|parent(H,M)_{T+\Delta T}^{i}\right) \quad (1)$$

It takes two steps to transform the DFT obtained above into DBN for subsequent calculation: the transformation of logic gates and the integration of DBNs. Section 3.2.1 lists 6 methods to transform 10 logic gates in human-machine systems. Section 3.2.2 specifically describes the integration of DBNs.

3.2.1. Transformation of logic gates

Directly converting a complete DFT to a DBN is a huge project, and there is basically no universal method for it. Generally, DFT has both dynamic logic gates and static logic gates [35], and the transformation of DFT to DBN is essentially the transformation of static and dynamic logic gates. The transformation method of various logic gates is given

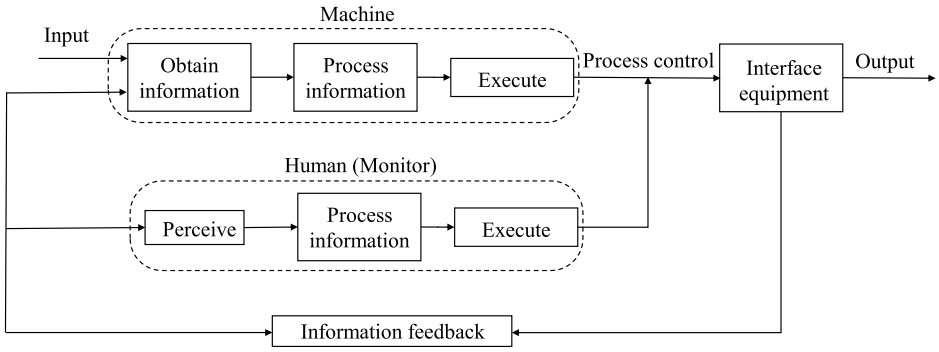


Fig. 3. An example of human-in-the-loop control diagrams.

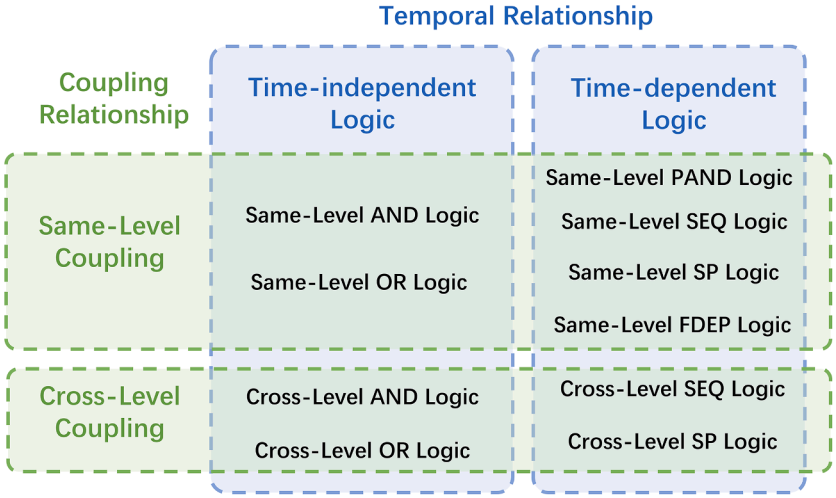


Fig. 4. Classification of logic between human errors and machine failures.

Table 2
Relationship between logic gates and logic in human-machine systems.

	Time-independent logic		Time-dependent logic	
	Same-level	Cross-level	Same-level	Cross-level
AND gate	√	√	—	—
OR gate	√	√	—	—
PAND gate	—	—	√	—
SEQ gate	—	—	√	√
SP gate	—	—	√	√
FDEP gate	—	—	√	—

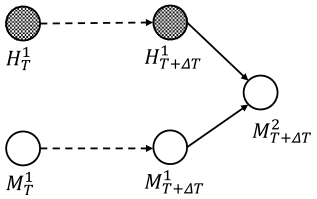
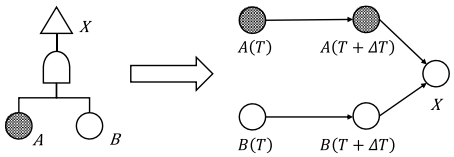


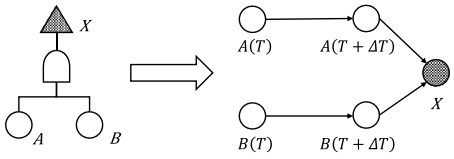
Fig. 5. A simplified example of DBN.

below. Suppose $X = 0$ indicates that fault X does not occur, $X = 1$ indicates that fault X occurs, and $f_X(t)$ indicates the probability density function of fault X. Since the hierarchical differences only causing variations in fault logic without affecting the transmission of conditional probabilities, the same type of logic across different hierarchical relationships can share a single transformation method. Thus, by employing 6 transformation methods, the conversion process of the 10 logics outlined in Section 3.1 can be adequately represented. It is worth noting that in all figures in this section, the nodes of the slash line represent human errors, and the white nodes represent machine failures.

1) Same-level AND / cross-level AND: These AND gates describe the logic that when all input events occur in human-machine systems, the output event will occur. It is applicable to the same-level and cross-level coupling relationships, so it includes both the same-level AND logic and the cross-level AND logic. Fig. 6 shows the AND gate and its corresponding DBN, and the CPD of nodes are listed in



(a). The same-level AND gate and its corresponding DBN



(b). One of the cross-level AND gate and its corresponding DBN

Fig. 6. The AND gates and their corresponding DBN.

Table 3
(a). The CPD of node $A(T+\Delta T)$ in the AND gates.

$A(T)$	$A(T+\Delta T)=1$	$A(T+\Delta T)=0$
1	1	0
0	$\int_T^{T+\Delta T} f_A(t)dt$	$1-\int_T^{T+\Delta T} f_A(t)dt$

Table 3(b). The CPD of node $B(T+\Delta T)$ in the AND gates

$B(T)$	$B(T+\Delta T)=1$	$B(T+\Delta T)=0$
1	1	0
0	$\int_T^{T+\Delta T} f_B(t)dt$	$1-\int_T^{T+\Delta T} f_B(t)dt$

Table 3(c). The CPD of node X in the AND gates

$A(T+\Delta T)$	$B(T+\Delta T)$	$X=1$	$X=0$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	1

Table 3. In Fig. 6(a), X can be a human error or machine failure at a higher level. Fig. 6(b) shows one case of the cross-level AND logic where nodes A and B are machine failures and node X is a human error at a higher level. The other case where A and B are human errors and X is a higher-level machine failure follows the same logic, so it is not repeatedly illustrated here.

2) Same-level OR / cross-level OR: The OR gates describe the logic that when any one of the input events occurs in human-machine systems, the output event will occur. It is applicable to the same-level and cross-level coupling relationships, so it includes both the same-level OR logic and the cross-level OR logic. Fig. 6 can also show the OR gate and its corresponding DBN. The CPD of nodes $A(T+\Delta T)$ and $B(T+\Delta T)$ are the same as those in the AND gate and the CPD of key node X is shown in Table 4.
3) Same-level PAND: The PAND gate describes the logic that the output event will occur only if the input events A and B both occur and A occurs before B. It is generally applicable to the same-level coupling relationship, so it only includes the same-level PAND logic. According to this sequential logic relationship, a two-state intermediate node Y needs to be added. $Y=1$ means that A occurs before B and $Y=0$ means that A does not occur before B. Either node A or node B is a human error, and the other is a machine failure. Node X can be any kind of higher-level fault. Fig. 7 shows one possibility of the PAND gate and its corresponding DBN. The CPD of key nodes $Y(T+\Delta T)$ and X are shown in Table 5.
4) Same-level SEQ / cross-level SEQ: The SEQ gates describe the logic that the input events occur in a certain order and cause the output event to occur. It is applicable to the same-level and cross-level coupling relationships, so it includes the same-level SEQ logic and the cross-level SEQ logic. In the same-level SEQ gate, one or more of nodes A, B, and C are human errors, and node X can be any kind of higher-level machine failure. In the cross-level SEQ gate, when nodes A, B, and C are all human errors, node X is a machine failure; when nodes A, B, and C are all machine failures, node X is a human error.

   Fig. 8 shows the SEQ gates and their corresponding DBN, where nodes A, B, and C must occur in turn before node X occurs. The CPD of the key nodes is shown in Table 6. Since the CPD of node $A(T+\Delta T)$ is the same as that in the AND gate and the CPD of node $C(T+\Delta T)$ is the same as that of $B(T+\Delta T)$, only the CPD of $B(T+\Delta T)$ is shown here.
5) Same-level SP / cross-level SP: the SP gates describe the logic that when the main part fails, the spare part starts to operate and replaces the main part. It is applicable to both the same-level and cross-level coupling relationships, so it includes both the same-level SP logic and the cross-level SP logic. According to whether there is any failure during the backup period of the spare part, the SP gate can be further divided into the cold spare (CSP) gate, the warm spare (WSP) gate, and the hot spare (HSP) gate. Since the CSP gate and the HSP gate can be regarded as special cases of the WSP gate, the discussion here focuses on the WSP gate. The WSP gate is the condition where the spare part probably fails during the backup period, but its failure rate is lower than that during the working period. The failure rate of the

Table 4
The CPD of node X in the OR gates.

$A(T+\Delta T)$	$B(T+\Delta T)$	$X=1$	$X=0$
1	1	1	0
1	0	1	0
0	1	1	0
0	0	0	1

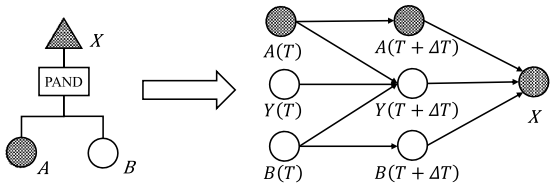


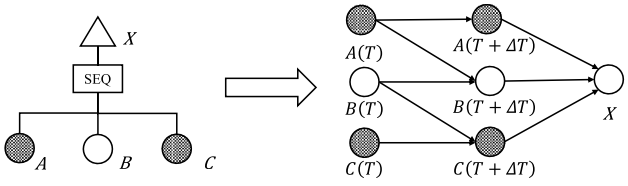
Fig. 7. The PAND gate and its corresponding DBN.

Table 5
(a). The CPD of node $Y(T+\Delta T)$ in the PAND gate.

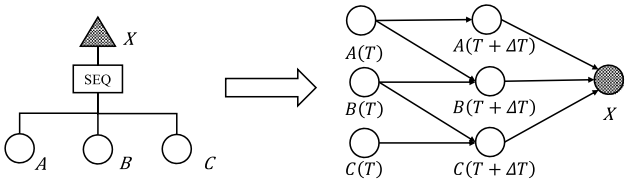
$A(T)$	$Y(T)$	$B(T)$	$Y(T+\Delta T)=1$	$Y(T+\Delta T)=0$
1	1	1	1	0
1	0	1	1	0
0	1	1	1	0
0	0	1	0	1
1	1	0	1	0
1	0	0	1	0
0	1	0	1	0
0	0	0	0	1

Table 5(b). The CPD of node X in the PAND gate

$A(T+\Delta T)$	$Y(T+\Delta T)$	$B(T+\Delta T)$	$X=1$	$X=0$
1	1	1	1	0
1	0	1	0	1
0	1	1	0	1
0	0	1	0	1
1	1	0	0	1
1	0	0	0	1
0	1	0	0	1
0	0	0	0	1



(a). One of the same-level SEQ gate and its corresponding DBN



(b). One of the cross-level SEQ gate and its corresponding DBN

Fig. 8. The SEQ gates and their corresponding DBN.

Table 6
(a). The CPD of node $B(T+\Delta T)$ in the SEQ gates.

$A(T)$	$B(T)$	$B(T+\Delta T)=1$	$B(T+\Delta T)=0$
1	1	1	0
1	0	$\int_T^{T+\Delta T} f_B(t)dt$	$1-\int_T^{T+\Delta T} f_B(t)dt$
0	1	0	1
0	0	0	1

Table 6(b). The CPD of node X in the SEQ gates

$A(T+\Delta T)$	$B(T+\Delta T)$	$C(T+\Delta T)$	$X=1$	$X=0$
1	1	1	1	0
1	0	1	0	1
0	1	1	0	1
0	0	1	0	1
1	1	0	0	1
1	0	0	0	1
0	1	0	0	1
0	0	0	0	1

spare part during the backup period is α, which is also called the dormancy factor, times the failure rate during the working period.

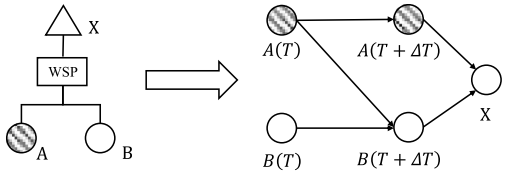
Fig. 9 shows the WSP gate and its corresponding DBN. The input event A on the left side of the WSP gate is specified as the main part, and B represents the spare part. The same-level WSP gate has a human error node and a machine failure node, and the node X can be any higher-level failure. The cross-level WSP gate has two machine failure nodes, and the node X is a higher-level human error node. The CPD of the key nodes is shown in Table 7. The $f_{BS}(t)$ is the failure probability density function of the spare part B during the backup period.

6) Same-level FDEP: The FDEP gate describes the logic that when a certain part in the system fails (or a trigger event occurs), the parts related to its function also fail. There is only the same-level FDEP logic in human-machine systems. X denotes trigger events, and A and B denote related events. All of these nodes can be human errors or machine failures. Fig. 10 shows one possibility of the FDEP gates and its corresponding DBN. The CPD of nodes $A(T+\Delta T)$ and $B(T+\Delta T)$ are the same in form, so only the CPD of $A(T+\Delta T)$ is listed in Table 8.

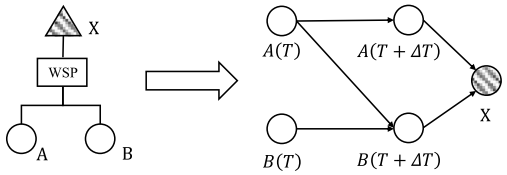
3.2.2. Integrating the DBN

The DBN directly transformed from the DFT by logic gates are usually fragmented, so a method of integrating the network fragments transformed from the DFT into a complete DBN is developed (Fig. 11).

This method includes the following steps. Take the bottom event in the DFT as the root node of the DBN and the remaining nodes in the network segment transformed from the DFT as leaf nodes. The root node



(a). One of the same-level WSP gate and its corresponding DBN



(b). The cross-level WSP gate and its corresponding DBN

Fig. 9. The WSP gates and their corresponding DBN.

Table 7
(a). The CPD of node $B(T+\Delta T)$ in the WSP gates.

$A(T)$	$B(T)$	$B(T+\Delta T)=1$	$B(T+\Delta T)=0$
1	1	1	0
1	0	$\int_T^{T+\Delta T} f_B(t)dt$	$1-\int_T^{T+\Delta T} f_B(t)dt$
0	1	1	0
0	0	$\int_T^{T+\Delta T} f_{BS}(t)dt$	$1-\int_T^{T+\Delta T} f_{BS}(t)dt$

Table 7(b). The CPD of node X in the WSP gates

$A(T+\Delta T)$	$B(T+\Delta T)$	$X=1$	$X=0$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	1

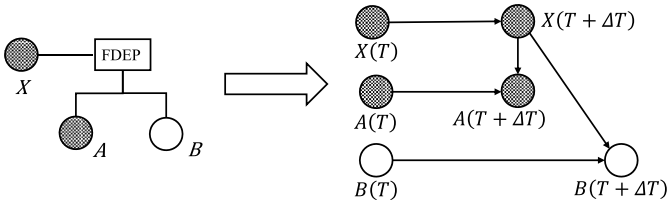


Fig. 10. The FDEP gate and its corresponding DBN.

Table 8
The CPD of node $A(T+\Delta T)$ in the FDEP gate.

$X(T+\Delta T)$	$A(T)$	$A(T+\Delta T)=1$	$A(T+\Delta T)=0$
1	1	1	0
1	0	1	0
0	1	1	0
0	0	$\int_T^{T+\Delta T} f_A(t)dt$	$1-\int_T^{T+\Delta T} f_A(t)dt$

and the leaf nodes are connected to obtain the initial network of the DBN. The transition network in the network segment transformed from the DFT is used as the transition network of the DBN. Finally, adjust the connections between the nodes according to the actual situation and expert experience and obtain the corresponding CPD. Now the DFT has been transformed into a complete DBN, which mainly includes two parts: the topology structure of the network and the corresponding CPD table. Through the aforementioned steps, the DFT describes the fault logic, while the DBN facilitates the easy calculation of the posterior probability of faults, thus achieving a critical transition between two different types of research content and research phases.

3.3. Simulation reasoning of DBN

The next step is to reason about the DBN. As a common DBN reasoning method, simulation has played an important role in recent years [36]. This paper selects the Gibbs sampling as the simulation method because it can be enhanced to efficiently obtain results while also reflecting the dynamic characteristics of the network.

First proposed in 1984, Gibbs sampling is an effective and simple simulation method [37]. It was applied to the probabilistic reasoning of static BNs shortly afterwards [14] and has become an important method for this kind of task. Gibbs sampling utilizes a set of complete conditional distributions for sampling. If there are n random variables, denoted by $X^1, X^2, \ldots, X^n$, then the conditional distribution formed like $p(x^i|x^j, j \neq i)$, $i = 1, 2, \ldots, n$ is called the complete conditional distribution. In Gibbs sampling, each complete conditional distribution is utilized to update different variables. Taking a static BN with n nodes as an example, two

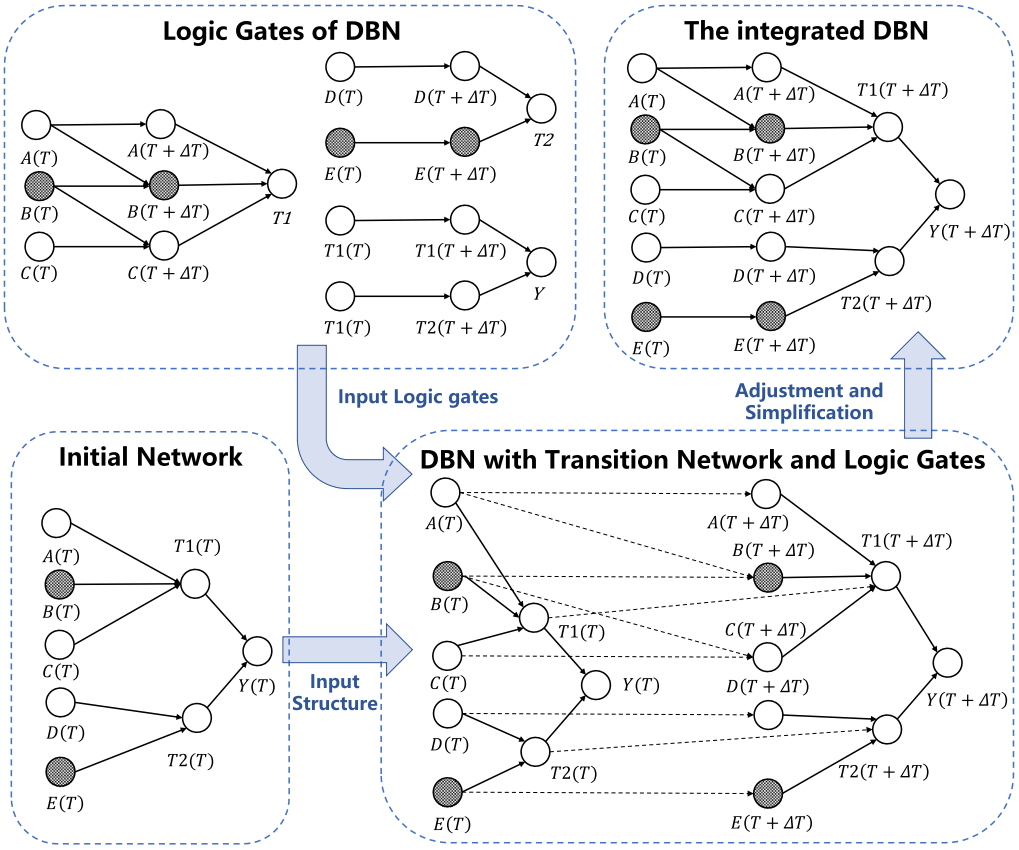


Fig. 11. Integrating network fragments transformed from the DFT into a DBN.

factors are considered: the n-dimensional node variables $V_1, V_2, ..., V_n$), and the length L of the Markov chain. The corresponding algorithm of Gibbs sampling is shown below:

Step 0: Initialization $v_0 = (v_0^1, v_0^2, ..., v_0^n)$;
Step 1: Sampling $v_1^1 \sim p(v^1 | v_0^2, v_0^3, ..., v_0^n)$;
Step 2: Sampling $v_1^2 \sim p(v^2 | v_1^1, v_0^3, ..., v_0^n)$;
Step 3: Sampling $v_1^3 \sim p(v^3 | v_1^1, v_1^2, ..., v_0^n)$;

…

Step *n*: Sampling $v_1^n \sim p(v^n | v_1^1, v_1^2, ..., v_1^{n-1})$

The transfer from v_0 to v_1 is completed in n steps. Later, by repeating Step1 ~ Step n for L times, a series of posterior samples can be obtained. According to these posterior samples, the relevant information of the posterior distribution can be calculated.

To apply the traditional Gibbs sampling to DBN, DBN needs to be expanded into a large-scale static BN on the time axis. Due to the addition of the new dimension (time), the entire algorithm requires one more loop.

Assuming that the DBN has T time slices, the number of steps for the entire algorithm is $L \times n \times T$. Taking a DBN of a human-machine system with T time slices and n nodes in each time slice as an example, the nodes are represented as $(H, M)^{ij}$, where i represents the time slice and j represents the j^{th} node in the time slice i. The algorithm of Gibbs sampling in DBN is shown below (the length of the Markov chain is L):

Step 0: Initialization

$$(H,M)_0 = ((H,M)_0^{11}, ..., (H,M)_0^{1n}, (H,M)_0^{21}, ..., (H,M)_0^{2n}, ..., (H,M)_0^{T1}, ..., (H,M)_0^{Tn}) \tag{2}$$

Step 1: Sampling

$$(H,M)_1^{11} \sim p\left((H,M)^{11} | (H,M)_0^{12} ..., (H,M)_0^{1n}, ..., (H,M)_0^{T1}, ..., (H,M)_0^{Tn}\right) \tag{3}$$

Step 2: Sampling

$$(H,M)_1^{12} \sim p\left((H,M)^{12} | (H,M)_1^{11}, (H,M)_0^{13}, ..., (H,M)_0^{1n}, ..., (H,M)_0^{T1}, ..., (H,M)_0^{Tn}\right) \tag{4}$$

Step *n*: Sampling

$$(H,M)_1^{1n} \sim p\left((H,M)^{1n} | (H,M)_1^{11} ..., (H,M)_1^{1(n-1)}, (H,M)_0^{21}, ..., (H,M)_0^{T1}, ..., (H,M)_0^{Tn}\right) \tag{5}$$

Step *n* + 1: Sampling

$$(H,M)_1^{21} \sim p\left((H,M)^{21} | (H,M)_1^{11} ..., (H,M)_1^{1n}, (H,M)_0^{22}, ..., (H,M)_0^{T1}, ..., (H,M)_0^{Tn}\right) \tag{6}$$

Step 2*n*: Sampling

$$(H,M)_1^{2n} \sim p\left((H,M)^{2n} | (H,M)_1^{11}, ..., (H,M)_1^{2(n-1)}, (H,M)_0^{31}, ..., (H,M)_0^{Tn}\right) \tag{7}$$

Step $T{\cdot}n$**:** Sampling

$$(H,M)_1^{Tn} \sim p\left((H,M)^{Tn}\middle|(H,M)_1^{11},\ldots,(H,M)_1^{1n},(H,M)_1^{21},\ldots,(H,M)_1^{T(n-1)}\right) \tag{8}$$

The transfer from $(H,M)_0$ to $(H,M)_1$ is completed in n steps. Later, by repeating Step1 ~ Step$T{\cdot}n$ L times, a series of posterior samples $(H,M)_1$, $(H,M)_2,\ldots,(H,M)_L$ can be obtained.

According to these posterior samples, the relevant information of the posterior distribution can be calculated. This posterior distribution information obtained by Gibbs sampling provides data for the significance analysis of human-machine systemic risk.

3.4. Importance analysis

According to the framework illustrated in Fig. 1, in the final stage of safety analysis, it is necessary to identify the critical human errors or machine failures leading to accidents by conducting importance analysis of the event nodes in the DBN. The results obtained from the simulation need to take node (human error or machine failure) importance analysis to identify the nodes that are most in need of improvement and optimization. Typically, certain metrics need to be defined to evaluate the results of PSA, which will facilitate the provision of importance rankings [38,39]. To illustrate the origins of these metrics, the risk function of node i in DBN is constructed as shown in Eq. (9). Where the independent variable E represents the probability of node fault occurrence, and b represents the probability of human-machine system fault in the scenario where node i remains entirely no fault, denoted as $P(Y=1|E_i=0)$.

$$Risk = a_i X_i + b_i \tag{9}$$

To better articulate Eq. (9), Fig. 12 is presented. Typically, the system fault probability at the current faultrate of node i is represented as $P(Y=1)$. When node i remains entirely free of faults, the system fault probability is denoted as $P(Y=1|E_i=0)$. The difference between $P(Y=1)$ and $P(Y=1|E_i=0)$ is termed as risk reduction (RR), which signifies the increment in system fault rate attributed to this node. Similarly, when node i is certain to experience a fault, the system fault probability is represented as $P(Y=1|E_i=1)$. The difference between $P(Y=1|E_i=1)$ and $P(Y=1)$ is termed as risk achievement (RA), denoting the worst-case scenario for system fault rate potentially induced by this node. By considering the three probabilities along the y-axis, RA, and RR, a series of importance analysis indicators can be constructed [40]. Certain suitable indicators are chosen to determine the ranking of node importance, or conducted based on the physical interpretations associated with these indicators.

Through logic analysis, DFT, DBN, simulation, and importance analysis, the safety analysis of human-machine systems is completed. The above safety analysis can be performed many times until the risk of the system meets the requirements.

4. Case study

4.1. Background

In order to verify the feasibility and effectiveness of the model, a case study of fuel filling is conducted. The fuel filling process is an important part, and its main function is to transport fuel according to the specified pressure and flow rate and provide propellant for the liquid rocket engine [41]. This process is a typical human-machine system [42]. In this paper, the fuel filling process will be simplified, and a liquid storage tank will be extracted for the case analysis, using this widely studied case to demonstrate the effectiveness of the method. Fig. 13 shows this process of fueling the rocket body from two hydrogen tanks [43].

It can be seen from the figure that the manual booster valves and the manual outlet valve need to be operated by operators. The vaporizer indicators, pumps, and the outlet valve are automatically controlled. All components in the system only have two states: fault and normal. Moreover, it is assumed that each component fails independently, cannot be repaired after fault, and features exponential distribution.

The major rules for the operation of the liquid storage tank system are as follows: the operator manually controls the booster valves to adjust the pressure in the hydrogen tank 1 and the hydrogen tank 2 according to the signal from the vaporizer indicators; the pumps adjust the flow of liquid hydrogen pumped into the rocket body to control the liquid level in the rocket body and balance the pressure in the two hydrogen tanks based on the liquid level signal and the vaporizer indicator signal; the outlet valve is responsible for outputting fuel. If the outlet valve fails, the operator controls the manual outlet valve to release the fuel.

In practice, the liquid hydrogen spill of the rocket body is a serious accident. Based on the method proposed in Section 3, the fault logic is delineated through the human-in-the-loop control diagram, then construct DFT and transformed into the corresponding DBN. Simulation is conducted to obtain the fault probabilities, and through importance indicators and analysis, identifies the critical nodes of the human-machine system safety.

4.2. Construction of DBN

First, the human-in-the-loop control diagram can be drawn according to the operating rules of the liquid storage tank, which can be divided into two parts. The first part is the operating rules of hydrogen tank 1 and hydrogen tank 2, including the operation of vaporizer indicators, manual booster valves, and pumps (Fig. 14). The second part is the operating rules of the outlet valves of rocket body (Fig. 15).

On the basis of the causal logic shown in Fig. 14 and Fig. 15, the DFT

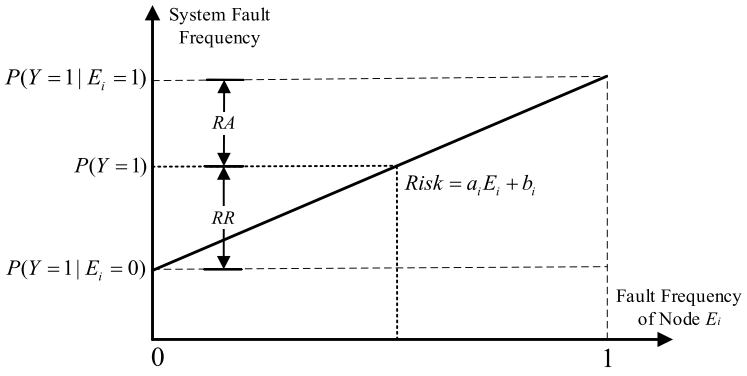


Fig. 12. Relationships of basic indicators in importance analysis.

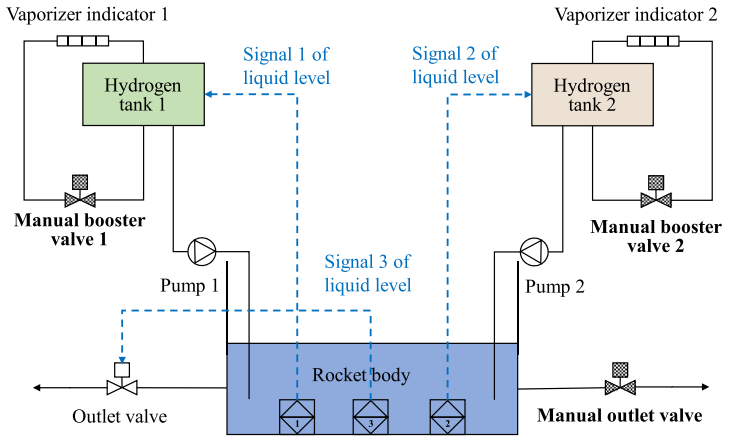


Fig. 13. The structure of the liquid storage tank.

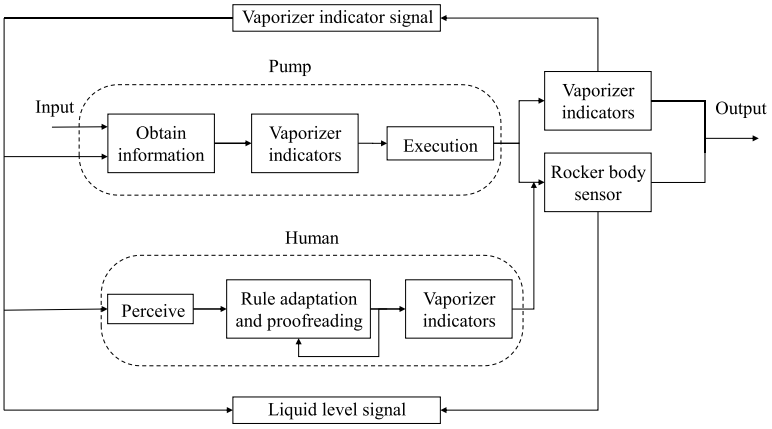


Fig. 14. The first part of the human-in-the-loop control diagram.

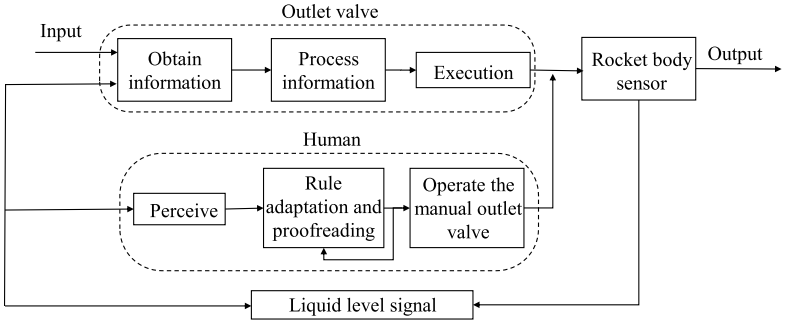


Fig. 15. The second part of the human-in-the-loop control diagram.

of the liquid storage tank system can be constructed. Table 9 shows the human errors and machine failures related to the liquid hydrogen spill accident and their failure rates. Due to the confidentiality of data in the space launch system and the versatility of the liquid storage tank case, the machine fault data and human error data in the table are general data. The machine failure data comes from the Offshore Reliability Data (OREDA), and the number of failures per thousand hours is regarded as the failure rate. The human error data comes from the International Atomic Energy Agency (IAEA) indicator system. The dormancy factor of WSP is selected as $\alpha = 0.8$ according to OREDA.

The complete DFT of the liquid storage tank system is shown in Fig. 16. This tank system consists of a WSP gate, two PAND gates, and four static gates. The human errors involved have been marked with slash lines. In this DFT, the manual outlet valve (the corresponding logic gate is the WSP gate) can be used as an example to show the relationship between the logic of fault in human-machine systems and the logic gate as well as the development of the DFT of the tank system. According to the logic shown in Fig. 15, the manual outlet valve is a spare part of the outlet valve, which will only be activated when the outlet valve fails. Since this switching process is operated by human, human error will be introduced. At this level, a machine failure (the failure of the outlet valve) occurs first, and a human error occurs while operating the spare part (manual outlet valve), resulting in a higher-level failure (the output flow of the rocket body is too small). This process is consistent with the

Table 9
Human errors and machine failures in the liquid hydrogen spill accident and their failure rates.

Symbols	Incidents	Failure rate ($1 \times 10^{-3}h^{-1}$)	Data resource
H1	Failure of manual outlet valve to open in time	3.37×10^{-2}	IAEA
H2	Incorrect opening of manual booster valve 1	2.61×10^{-2}	IAEA
H3	Incorrect opening of manual booster valve 2	2.61×10^{-2}	IAEA
M1	Fault of outlet valve	1.67×10^{-3}	OREDA
M2	Fault of vaporizer indicator 1	3.12×10^{-2}	OREDA
M3	Fault of pump 1	4.10×10^{-2}	OREDA
M4	Fault of pump 2	4.10×10^{-2}	OREDA
M5	Fault of vaporizer indicator 2	3.12×10^{-2}	OREDA
S1	Small output flow of rocket body	—	—
S2	Large output flow of rocket body	—	—
T1	Large output flow of liquid hydrogen 1	—	—
T2	Large output flow of liquid hydrogen 2	—	—
X1	Large pressure of hydrogen storage tank 1	—	—
X2	Large pressure of hydrogen storage tank 2	—	—
Y	Liquid hydrogen spill accident of rocket body	—	—

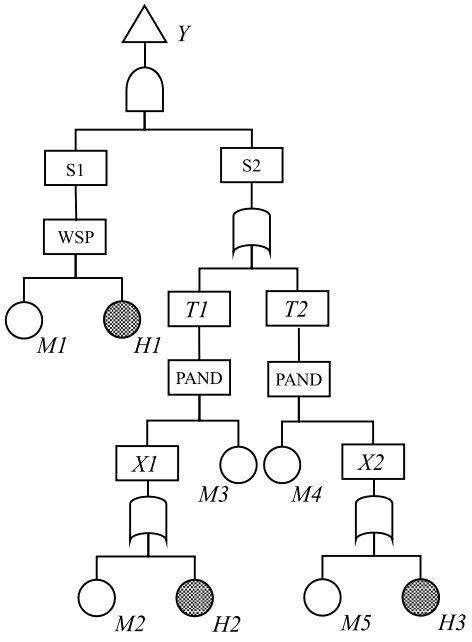


Fig. 16. DFT of liquid hydrogen spill accident in rocket body.

same-level SP logic of human-machine systems, so it can be described by the WSP gate.

According to the method proposed in 3.2, the DFT is further transformed into a DBN to quantitatively calculate the probability of the accident (Fig. 17). In this network, the human error nodes are marked with slash lines, and Q1 and Q2 are the intermediate nodes of the PAND gate.

4.3. Reasoning of DBN

Based on the dynamic Bayesian simulation method, the BNT toolbox is utilized to construct a DBN containing 10 time slices (the unit of time is 1000 h), and Gibbs sampling is utilized to perform probabilistic

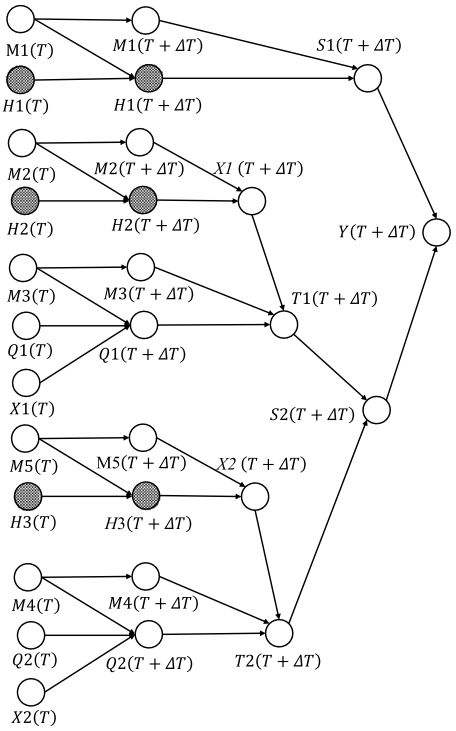


Fig. 17. DBN of liquid hydrogen spill accident in rocket body.

reasoning to the DBN of the liquid storage tank system. All human errors and machine failures data utilized in the simulation are derived from the information presented in Table 9 of Section 4.2. In order to analyze the accuracy and time performance of the Gibbs sampling method, a commonly used precise reasoning algorithm—the junction tree algorithm—is selected for comparison. Its basic idea is to transform the BN into a junction tree structure through graph conversion, then use a series of cliques to perform reasoning, and finally achieve global consistency for the whole junction tree [44].

The failure probability of each node at the initial moment is set as 0. 100 sets of data for each node are selected to calculate its average value, which is regarded as the probability of that node. Finally, the reasoning results of the liquid hydrogen spill accident of the rocket body are shown in Table 10. The values in the table represent the probabilities ($P(Y_t = 1)$) of the top event (Liquid hydrogen spill accident of rocket body) occurring over time as calculated by the simulation method. Fig. 18 shows the trend in probability over time and the time required for a single reasoning of the two reasoning methods.

It can be clearly seen from Fig. 18 that the probability of the liquid hydrogen spill accident gradually increases with time, reflecting the dynamic characteristics of the human-machine system. In addition, the two curves in Fig. 18 do not completely overlap, indicating that Gibbs sampling still suffers from a certain degree of error compared with the selected precise reasoning algorithm. In this example, the minimum error rate is 0 and the maximum error rate reaches 11.7 %. However, compared with the junction tree algorithm, the Gibbs sampling algorithm saves about 92 % of the time for a single reasoning and has a

Table 10
Simulation-Based $P(Y_t = 1)$ of the liquid hydrogen spill accident of rocket body.

Time (h)	0	1000	2000	3000	4000
Junction Tree	0	0.0113	0.0131	0.0154	0.0183
Gibbs Sampling	0	0.0113	0.0123	0.0150	0.0160
Time (h)	5000	6000	7000	8000	9000
Junction Tree	0.0215	0.0251	0.0291	0.0332	0.0375
Gibbs Sampling	0.0193	0.0230	0.0280	0.0349	0.0419

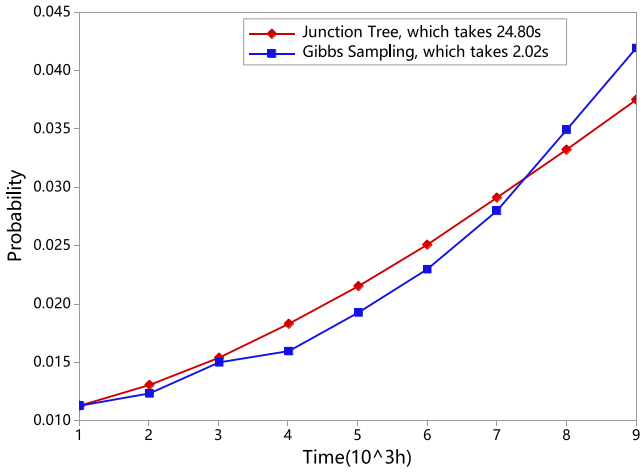


Fig. 18. Comparison of Gibbs sampling and the junction tree algorithm in probability over time.

greater time performance, so this error rate is acceptable in practice. Finally, from the perspective of safety analysis, although the probability of a liquid hydrogen spill accident gradually increases over time, it has always been maintained at a relatively low level, which means the liquid storage tank system has a high level of safety.

4.4. Importance analysis of the case

Based on the results obtained by sampling, the importance of each node needs to be analyzed with reasonable indicators [38]. In this paper, three indicators are selected to construct an importance analysis scheme: probability importance (PI), risk reduction worth (RRW) and risk achievement worth (RAW).

PI represents the degree of change in the probability of leaf node fault caused by the change in the root node's state. RRW represents the ratio of the leaf node fault probability to the leaf node fault probability when the root node is in the normal state. In contrast, RAW denotes the ratio of the leaf node failure probability when the root node is in the failure state to the leaf node failure probability. Their mathematical expression is shown in Eq. (10) Eq. (11) and Eq. (12). Where$E_i$represents the state of the root node E_i at time t, and Y_t represents the state of the leaf node Y at time t.

$$PI_{E_i,Y_t} = \frac{P(Y_t = 1|E_i = 1)}{P(Y_t = 1|E_i = 0)} \tag{10}$$

$$\mathrm{RRW}_{E_i,Y_t} = \frac{P(Y_t = 1)}{P(Y_t = 1|E_i = 0)} \tag{11}$$

$$\mathrm{RAW}_{E_i,Y_t} = \frac{P(Y_t = 1|E_i = 1)}{P(Y_t = 1)} \tag{12}$$

To study the impact of each root node on the final leaf node, an importance analysis of each node is carried out with PI, RRW and RAW as indicators of the impact of node fault on the system safety. 2000 h of data is selected for calculation and the results are presented in Table 11 and Fig. 19. The data are derived from Table 9 in Section 4.2, representing the failure probabilities of each bottom-level node. The simulation is conducted according to the process outlined in Section 3.3, and the simulation results are computed based on Eqs. (10) to (12). For example, in Table 11, the values of PI, RRW, and RAW are calculated based on $P(Y_{2000} = 1|E_{ti} = 1)$ and $P(Y_{2000} = 1|E_{ti} = 0)$, as well as the $P(Y_{2000} = 1)$ from Table 10. Fig. 19 visually presents the calculated results of PI, RRW, and RAW for each node.

By observing the results of the importance analysis of the root node,

Table 11
Results of conditional probabilities and importance for each node at 2000 h.

Node	$P(Y_{2000} = 1\|E_{ti} = 1)$	$P(Y_{2000} = 1\|E_{ti} = 0)$	PI	RRW	RAW
H1	0.0140	0.0125	1.1200	1.0480	1.0687
H2	0.0136	0.0130	1.0462	1.0077	1.0382
H3	0.0139	0.0127	1.0945	1.0315	1.0611
M1	0.0136	0.0118	1.1525	1.1102	1.0382
M2	0.0138	0.0129	1.0698	1.0155	1.0534
M3	0.0139	0.0121	1.1488	1.0826	1.0611
M4	0.0134	0.0123	1.0894	1.0650	1.0229
M5	0.0137	0.0122	1.1230	1.0738	1.0458

it can be found that within the portion where each indicator value exceeds 1, PI approximates the sum of RRW and RAW. This needs to be explained in the context of the significance of these indicators. In the intervals depicted in Fig. 12, the PI evaluates the entire range from $P(Y = 1|E_i = 0)$ to $P(Y = 1|E_i = 1)$. This interval is comprised of the range from $P(Y = 1|E_i = 0)$ to $P(Y = 1)$, where RRW is located; and the range from $P(Y = 1)$ to $P(Y = 1|E_i = 1)$, where RAW is located. In this way, the three indicators can be interpreted as follows: PI signifies the magnitude of system fault probability change caused by the node, RRW denotes the optimization potential of the node, and RAW represents the degradation potential of the node.

From the meaning of the above indicators, two methods of importance analysis can be derived. The first way is comparing the PI values of each node, as larger PI values indicate that the node can cause a greater change in the system's fault rate. Therefore, optimization can begin with node having the highest PI values. The second way is comparing the magnitudes of RRW and RAW for each node. When RRW exceeds RAW, it indicates that the node currently resides in a higher position within the range from $P(Y = 1|E_i = 0)$ to $P(Y = 1|E_i = 1)$, signifying a larger optimization potential. Additionally, the greater the difference between RRW and RAW, the larger the optimization space, thus indicating a higher degree of worthiness for optimization. Conversely, if RAW exceeds RRW, the optimization space for the node is smaller, resulting in a lower level of importance.

In the following analysis, we can consider both of these approaches to interpret the results in Fig. 19. From the perspective of PI values, it can be observed that the nodes M1 (Fault of outlet valve) and M3 (Fault of pump 1) hold the highest importance, with values of 1.1525 and 1.1488 respectively. followed by nodes M5 (Fault of vaporizer indicator 2) and H1 (Fault of manual outlet valve to open in time), with values of 1.1230 and 1.1200 respectively. Analyzing the difference between RRW and RAW reveals that nodes M1, M4 (Fault of pump 2), and M5 are relatively more important. Taking both approaches into consideration, node H1 has a lower PI value compared to other nodes, indicating a smaller potential for optimization, and thus lower priority. Additionally, it is observed that node M4 shares similarities with node M3 in both structure and fault logic, making it possible to prioritize the more urgent optimization of node M3 and then transfer the optimization experience to node M4. Consequently, the current round of optimization should focus on nodes M1, M3, and M5. Among them, M1 (Fault of outlet valve) holds the highest importance in both evaluation approaches, rendering it the weakest node in the system.

This case analysis proves the feasibility of the dynamic Bayesian simulation method. The probability of the liquid hydrogen spill accident of the rocket body increases over time but generally remains at a low level, which proves that the liquid storage tank system is basically safe, but there is still a need to optimize and improve certain critical nodes. After conducting a comparative analysis using the three indicators PI, RRW, and RAW, it is evident that nodes M1, M3, and M5 are the most critical nodes requiring optimization. Among them, M1 represents the weakest point within the liquid storage tank system, requiring enhance its operating process or environment to improve the overall safety of the system.

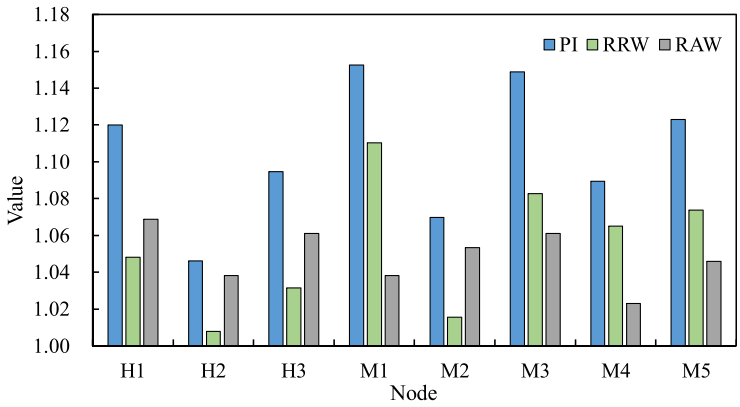


Fig. 19. Values of PI, RRW, and RAW for each node.

The dynamic Bayesian simulation method emphasizes continuous improvement throughout the system's life cycle. In this case, after optimizing nodes M1, M3, and M5, a subsequent simulation can be performed to calculate the optimized system's fault probability $P(Y=1)$ and determine if it meets the system requirements. If the requirements are not met, another round of nodes importance analysis is conducted, and optimization is carried out based on the analysis results. This iterative optimization process continues until the overall system fault probability meets the specified requirements.

4.5. Case discussion

The reason why human-machine systems become dynamic is mostly because of humans. The abundant and complex human-machine interactions in human-machine systems endow the system with dynamic characteristics. Therefore, humans are as crucial as machines in the safety analysis of human-machine systems and require detailed research. Following this approach, this paper places humans and machines on an equal footing, investigates the fault logic within human-machine systems, and proposes the dynamic Bayesian simulation method for evaluating the safety of human-machine systems. To validate the method, this section selects a typical human-machine system - the fuel filling process in space launches. Through human-in-the-loop control analysis, construction of DFT, conversion from DFT to DBN, Gibbs sampling simulation, and importance analysis, critical nodes affecting the human-machine system are identified, laying the foundation for subsequent system safety enhancements.

Through the case study, this paper makes the following two findings: (1) Expressing the logic of human-machine relationships in human-machine systems is extremely challenging. This is because the interaction between humans and machines in human-machine systems is often widespread, with evident temporal and hierarchical relationships. For example, in the fuel filling process during space launches, there exists feedback and self-looping between humans and machines, making it difficult for traditional analytical methods to extract the logic. Therefore, more advanced logic analysis methods are needed to analyze human-machine systems. This paper conducts the analysis from the perspective of system control and draws control diagrams of human-machine systems. Subsequently, by designing hierarchical and temporal logics, the logic in human-machine systems is classified. The method proposed in this paper can clearly express the coupling logic in human-machine systems, demonstrating rationality and comprehensiveness. (2) The refined DBN structure is clear, capable of representing various coupling relationships in human-machine systems, providing support for the accuracy of subsequent calculations and solutions. Depending on the scale, DBN networks can be accurately solved using methods such as Junction Tree, or simulated using techniques like Gibbs sampling. Among these methods, Gibbs sampling significantly reduces solving time while maintaining precision at a relatively small decrease, thus offering high efficiency. Following the solving process, targeted importance analysis can be conducted to identify critical nodes for system safety.

Furthermore, it is noteworthy that the failure rates of each node in this case study are based on authoritative database data. However, in practical human-machine system case analyses, historical failure data is often used to calculate failure rates. The lack or distortion of historical data often leads to data uncertainty, which is a problem that must be addressed when applying the method in practice. In such cases, appropriate importance analysis indicators can be chosen based on the tendency of data uncertainty to correct the data to some extent. For example, when the original data are significantly higher than the true values, risk reduction-related indicators can be used for correction; conversely, risk achievement-related indicators can be chosen for correction. Existing literature has extensively studied these indicators [40]. Additionally, fuzzy mathematics or grey system theory can be employed to whiten the data in practical human-machine systems, thereby obtaining more accurate and reliable failure rates data [45,46]. These methods effectively address the issue of data uncertainty in human-machine systems, providing references for ensuring the accuracy of the method's practical application.

The case and the discussion above illustrate three advantages of the dynamic Bayesian simulation method. Firstly, it considers machine failures and human errors in detail and utilizes various data for safety analysis. Secondly, it is good at characterizing the uncertainty and dynamics of human-machine systems. Finally, this method saves a lot of time and increases the feasibility of continuous improvement of the system, which is a great advantage for applications in engineering.

5. Conclusion

Quantitative safety analysis of human-machine systems faces challenges as these systems grow more complex and feature dynamic human-machine coupling relationships. Traditional methods often fail to elucidate this coupling logic and involve computationally intensive direct modeling. In contrast, the dynamic Bayesian simulation method proposed in this paper offers a more effective solution for human-machine system safety assessment.

By analyzing the system's fault mechanisms from a control perspective, it establishes 10 types of logic between human errors and machine failures, demystifying the human-machine coupling relationship in safety analysis. Constructing the human-machine system's DFT based on this fault logic, followed by transforming it into a DBN, circumvents the challenges of directly establishing complex DBN and avoids the combinatorial explosion problem inherent in DFTs. During DBN simulation, the extended Gibbs sampling technique is employed to optimize system reasoning time while ensuring accuracy. Based on the

simulation results, this paper discusses methods for setting safety analysis indicators, allowing for the selection of more complex indicators based on the requirements of specific cases. Through a case study of the fuel filling process in space launches, the method identifies the "Fault of outlet valve" as the weakest node in the current human-machine system safety, paving the way for future rocket filling system improvements.

In summary, the dynamic Bayesian simulation method facilitates rapid safety analysis and continuous enhancement of human-machine systems by pinpointing risks and weak points in each node. It is of great practical value in engineering for its better information utilization, dynamic representation, and time performance. Future research could delve deeper into human-machine system fault logic, considering factors such as human situational awareness, to further refine its applications.

CRediT authorship contribution statement

Xing Pan: Writing – review & editing, Writing – original draft, Supervision, Project administration, Methodology, Funding acquisition, Conceptualization. **Hengte Du:** Writing – review & editing, Visualization, Methodology, Formal analysis, Conceptualization, Writing – original draft. **Haofan Yu:** Methodology, Data curation, Conceptualization, Software, Writing – original draft.

Declaration of competing interest

The author(s) declared no potential conflicts of interest with respect to the research, author- ship, and/or publication of this article.

Data availability

Data will be made available on request.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under grant No. 72071011.

References

[1] Zeng Z, Barros A, Coit D. Dependent failure behavior modeling for risk and reliability: a systematic and critical literature review. Reliability Engineering & System Safety; 2023, 109515.
[2] Li PC, Chen GH, Dai LC, Zhang L. A fuzzy Bayesian network approach to improve the quantification of organizational influences in HRA frameworks. Saf. Sci. 2012; 50(7):1569–83. https://doi.org/10.1016/j.ssci.2012.03.017.
[3] Guan W, Liu Q, Dong C. Risk assessment method for industrial accident consequences and human vulnerability in urban areas. J. Loss Prev. Process Ind. 2022;76:104745. https://doi.org/10.1016/j.jlp.2022.104745.
[4] Yazdi M, Nedjati A, Zarei E, Abbassi R. A novel extension of DEMATEL approach for probabilistic safety analysis in process systems. Saf. Sci. 2020;121:119–36. https://doi.org/10.1016/j.ssci.2019.09.006.
[5] Mansikka H, Harris D, Virtanen K. Pilot competencies as components of a dynamic human-machine system. Hum. Factors Ergon. Manuf. Serv. Ind. 2019;29(6): 466–77.
[6] Fu C, Sayed T. Bayesian dynamic extreme value modeling for conflict-based real-time safety analysis. Analytic methods in accident research 2022;34:100204. https://doi.org/10.1016/j.amar.2021.100204.
[7] Han S, Wang T, Chen J, Wang Y, Zhu B, Zhou Y. Towards the human–machine interaction: strategies, design, and human reliability assessment of crews' response to daily cargo ship navigation tasks. Sustainability 2021;13(15):8173. https://doi.org/10.3390/su13158173.
[8] Chickering M, Heckerman D, Meek C. Large-sample learning of Bayesian networks is NP-hard. J. Mach. Learn Res. 2004;5:1287–330. https://doi.org/10.1023/B:JODS.0000045365.56394.b4.
[9] Kabir S, Papadopoulos Y. Applications of Bayesian networks and Petri nets in safety, reliability, and risk assessments: a review. Saf. Sci. 2019;115:154–75. https://doi.org/10.1016/j.ssci.2019.02.009.
[10] Zio E. Integrated deterministic and probabilistic safety assessment: concepts, challenges, research directions. Nucl. Eng. Des. 2014;280:413–9. https://doi.org/10.1016/j.nucengdes.2014.09.004.
[11] Park JW, Lee SJ. Simulation optimization framework for dynamic probabilistic safety assessment. Reliab. Eng. Syst. Saf. 2022;220:108316. https://doi.org/10.1016/j.ress.2021.108316.
[12] Vesely WE, Goldberg FF, Roberts NH, Haasl DF. Fault tree handbook. Washington DC: Nuclear Regulatory Commission; 1981.
[13] Xiong S, Yingfu G, Huan Y, et al. Reliability study of motor controller in electric vehicle by the approach of fault tree analysis. Eng Fail Anal 2021;121:105165.
[14] Pearl J. Evidential reasoning using stochastic simulation of causal models. Artif. Intell. 1987;32(2):245–57. https://doi.org/10.1016/0004-3702(87)90012-9.
[15] Tosin A, Mahmood S, Enrico Z. Bayesian Network Modelling for the Wind Energy Industry: An Overview. Reliab Eng Syst Saf 2020;202:107053.
[16] Xu W, Wang TK. Dynamic safety prewarning mechanism of human–machine–environment using computer vision. Engineering, Construction and Architectural Management; 2020. https://doi.org/10.1108/ECAM-12-2019-0732.
[17] Yu H, Wu X. A method for transformation from dynamic fault tree to binary decision diagram. Proceedings of the Institution of Mechanical Engineers, Part O: *Journal of Risk and Reliability* 2021;235(3):416–30. https://doi.org/10.1177/1748006×20974187.
[18] Omar K, Paolo G, Gian PC. Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks. Reliab Eng Syst Saf 2020;198:106813.
[19] Zand R, Camsari KY, Pyle SD, Ahmed I, Kim CH, DeMara RF. Low-energy deep belief networks using intrinsic sigmoidal spintronic-based probabilistic neurons. In: Proceedings of the 2018 on Great Lakes Symposium on VLSI; 2018. p. 15–20. https://doi.org/10.1145/3194554.3194558.
[20] Zhou S, Xiang J, Wong WE. Reliability analysis of dynamic fault trees with spare gates using conditional binary decision diagrams. Journal of Systems and Software 2020;170:110766. https://doi.org/10.1016/j.jss.2020.110766.
[21] Aghaei P., Asadollahfardi G., Katabi A. Safety risk assessment in shopping center construction projects using Fuzzy Fault Tree Analysis method. Quality & Quantity 2021:2.
[22] Havlikova M, Jirgl M, Bradac Z. Human reliability in man-machine systems. Procedia Eng 2015;100:1207–14. https://doi.org/10.1016/j.proeng.2015.01.485.
[23] Lu Q, Zhang W. Integrating dynamic Bayesian network and physics-based modeling for risk analysis of a time-dependent power distribution system during hurricanes. Reliab Eng Syst Saf 2022;220:108290.
[24] Reid T, Gibert J. Inclusion in human–machine interactions. Science 2022;375 (6577):149–50. https://doi.org/10.1126/science.abf2618.
[25] Hirose T., Sawaragi T., Nomoto H., et al. Functional safety analysis of SAE conditional driving automation in time-critical situations and proposals for its feasibility. Cognition, Technology & Work 2020:1–19.
[26] Lavrov E, Siryk O, Volosiuk A, Zolkin A, Sedova N. Sustainability and reliability ensurance models for automated technological systems in chemical industry: systemic ergonomic approach. In: E3S Web of Conferences. 280. EDP Sciences; 2021. p. 02005.
[27] Brisco NDA, Wolfgang N, Serge DY. Machine reliability optimization by genetic algorithm approach. Global Journals of Research in Engineering 2020;20(A2): 35–40. https://doi.org/10.34257/GJREAVOL20IS2PG35.
[28] Yen TC, Wang KH, Wu CH. Reliability-based measure of a retrial machine repair problem with working breakdowns under the F-policy. Comput. Ind. Eng. 2020; 150:106885. https://doi.org/10.1016/j.cie.2020.106885.
[29] Wang Z, Zeng S, Guo J, Che H. A Bayesian network for reliability assessment of man-machine phased-mission system considering the phase dependencies of human cognitive error. Reliab. Eng. Syst. Saf. 2021;207:107385. https://doi.org/10.1016/j.ress.2020.107385.
[30] Amaya-Toral RM, Piña-Monarrez MR, Reyes-Martínez RM, et al. Human–Machine Systems Reliability: A Series–Parallel Approach for Evaluation and Improvement in the Field of Machine Tools. Appl Sci 2022;12(3):1681.
[31] Li C, Mahadevan S. Efficient approximate inference in Bayesian networks with continuous variables. Reliab. Eng. Syst. Saf. 2018;169:269–80. https://doi.org/10.1016/j.ress.2017.08.017.
[32] Che H, Zeng S, Guo J. Reliability assessment of man-machine systems subject to mutually dependent machine degradation and human errors. Reliab. Eng. Syst. Saf. 2019;190:106504. https://doi.org/10.1016/j.ress.2019.106504.
[33] Murphy KP. Dynamic bayesian networks: representation, inference and learning. University of California, Berkeley; 2002.
[34] Zhao Y, Tong J, Zhang L, Wu G. Diagnosis of operational failures and on-demand failures in nuclear power plants: an approach based on dynamic Bayesian networks. Ann. Nucl. Energy 2020;138:107181. https://doi.org/10.1016/j.anucene.2019.107181.
[35] Dugan JB, Bavuso SJ, Boyd MA. Dynamic fault-tree models for fault-tolerant computer systems. IEEE Trans. Reliab. 1992;41(3):363–77. https://doi.org/10.1109/24.159800d.
[36] Kelleher CT, Hill RR, Bauer KW, Miller JO. Using dynamic Bayesian networks as simulation metamodels based on bootstrapping. Comput. Ind. Eng. 2018;115: 595–602. https://doi.org/10.1016/j.cie.2017.11.033.
[37] Geman S, Geman D. Stochastic relaxation, gibbs distributions, and the bayesian restoration of images. IEEE Transactions on pattern analysis and machine intelligence; 1984. p. 721–41. https://doi.org/10.1109/TPAMI.1984.4767596.
[38] He L, Lu Z, Li X. Failure-mode importance measures in structural system with multiple failure modes and its estimation using copula. Reliab. Eng. Syst. Saf. 2018; 174:53–9. https://doi.org/10.1016/j.ress.2018.02.016.
[39] Xie M, Goh TN, Mahmood T. Statistical models for monitoring the high-quality processes. Springer handbook of engineering statistics. London: Springer London; 2023. p. 261–74.
[40] Van der Borst M, Schoonakker H. An overview of PSA importance measures. Reliab. Eng. Syst. Saf. 2001;72(3):241–5.

[41] Pan X, Zuo D, Zhang W, Hu L, Wang H, Jiang J. Research on human error risk evaluation using extended Bayesian networks with hybrid data. Reliab. Eng. Syst. Saf. 2021;209:107336. https://doi.org/10.1016/j.ress.2020.107336.
[42] Haber JM. Launch and reentry safety objectives. Journal of Space Safety Engineering 2017;4(1):22–8. https://doi.org/10.1016/j.jsse.2017.03.006.
[43] Hu Y, Parhizkar T, Mosleh A. Guided simulation for dynamic probabilistic risk assessment of complex systems: concept, method, and application. Reliab Eng Syst Saf 2022;217:108047.
[44] Lauritzen SL, Spiegelhalter DJ. Local computations with probabilities on graphical structures and their application to expert systems. J. R. Stat. Soc. Series B Stat. Methodol. 1988;50(2):157–94. https://doi.org/10.1111/j.2517-6161.1988.tb01721.x.
[45] Yang Y, John R. Grey sets and greyness. Inf Sci (Ny) 2012;185(1):249–64. https://doi.org/10.1016/j.ins.2011.09.029.
[46] Zadeh LA. Fuzzy sets. Information & Control 1965;8(3):338–53. https://doi.org/10.1016/S0019-9958(65)90241-X.