An integrated approach to quantitative resilience assessment in process systems

Sun, Hao; Yang, Ming; Wang, Haiqing

DOI
10.1016/j.ress.2023.109878

Publication date
2024

Document Version
Final published version

Published in
Reliability Engineering and System Safety

Citation (APA)
Sun, H., Yang, M., & Wang, H. (2024). An integrated approach to quantitative resilience assessment in process systems. *Reliability Engineering and System Safety*, *243*, Article 109878. https://doi.org/10.1016/j.ress.2023.109878

Reliability Engineering and System Safety 243 (2024) 109878

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

An integrated approach to quantitative resilience assessment in process systems

Hao Sun [a,b,c,*], Ming Yang [b], Haiqing Wang [c]

[a] *School of Civil Engineering and Architecture, Anhui University of Technology, Maanshan, Anhui 243002, China*
[b] *Safety and Security Science Section, Department of Values, Technology, and Innovation, Faculty of Technology, Policy, and Management, Delft University of Technology, the Netherlands*
[c] *College of Mechanical and Electronic Engineering, China University of Petroleum (East China), Qingdao, China*

ARTICLE INFO

Keywords:
Process safety
Human-technical systems, FRAM, resilience

ABSTRACT

Chemical process systems are becoming more automated and complex, which leads to increased interaction and interdependence between the human and technical elements of process systems. This urges the need for updating the safety assessment method by treating “safety” as an emergent property of a system. Uncertainty comes together with complexity. To enhance system ability of dealing with uncertain disruptions, this paper proposes a quantitative resilience assessment method by modeling the failure propagation (initiated by a disruption) across the functional units of a system. The Functional Resonance Analysis Method (FRAM) is utilized to model the system operation to represent the relationship among its function units and to consider the interactions among human-technical factors. Then, a Cascading Failure Propagation Model (CFPM) is developed to quantify the fault propagation process and reflect the system functionality changes over time for resilience assessment. The proposed method is applied to a propane-feeding control system. The results show that it can help practitioners understand the process of fault propagation and risk increase, identify potential ways to design a more resilient system to respond to uncertain disruptions/attacks, and provide a real-time dynamic resilience profile to support decision-making.

1. Introduction

Chemical process systems store and process large amounts of hazardous materials, which may lead to casualties, extreme property damage, and ecological pollution [1–3]. For example, the Amuay refinery disaster in Venezuela caused more than 50fatalities, over 100 people injured, and about 1600 buildings destroyed, resulting in $1 billion in economic loss [4].

To prevent accidents, risk assessment (RA) methods and safety-enhancing measures were developed to reduce the probability of an accident and mitigate accident consequences [5,6]. RA plays an essential role in understanding the mechanism of accidents and ensuring system safety [7,8]. O’Connor et al. [9] proposed three crucial elements of safety, namely, prevention, mitigation, and response, which can be integrated as a so-called safety triad. These three factors may seem simple, even intuitive. However, reports and investigations of accidents have proven that the leading cause of accidents was the lack of foresight and the weakness of these three factors [10]. Degradation, common cause failures, and other dependencies are overlooked or neglected. Risk analysis developed further, though. Ghosh et al. [11] utilized a copula-based Bayesian network (BN) and traditional BN to assess the failure of the multivariable time-dependent system. Mamudu et al. [12] proposed a comprehensive method, which consists of a multilayer perceptron–artificial neural network (ANN) and BN, to assess the risk of the system. Zarei et al. [13] used Bow–tie and BN to analyze system risk. Sun et al. [14] developed an integrated approach based on the window of opportunity and complex network to evaluate the risk of a process system.

The works described above show the significant progress in RA of process systems. Nevertheless, recurring accidents show that relying on RA alone to identify and counter hazards is insufficient to ensure system safety [15]. Nowadays, systems tend to become more complex to meet market demand so that non-linear interdependencies, tight coupling, and possibly dysfunctional components failure, as Perrow (1984) observed, may exhibit more frequently. Ensuing uncertainty, complex interaction, and interdependence between components (e.g., human,

* Corresponding author at: School of Civil Engineering and Architecture, Anhui University of Technology, Maanshan, Anhui 243002, China.
E-mail address: sunhao_upc@outlook.com (H. Sun).

https://doi.org/10.1016/j.ress.2023.109878
Received 20 November 2022; Received in revised form 12 July 2023; Accepted 8 December 2023
Available online 13 December 2023

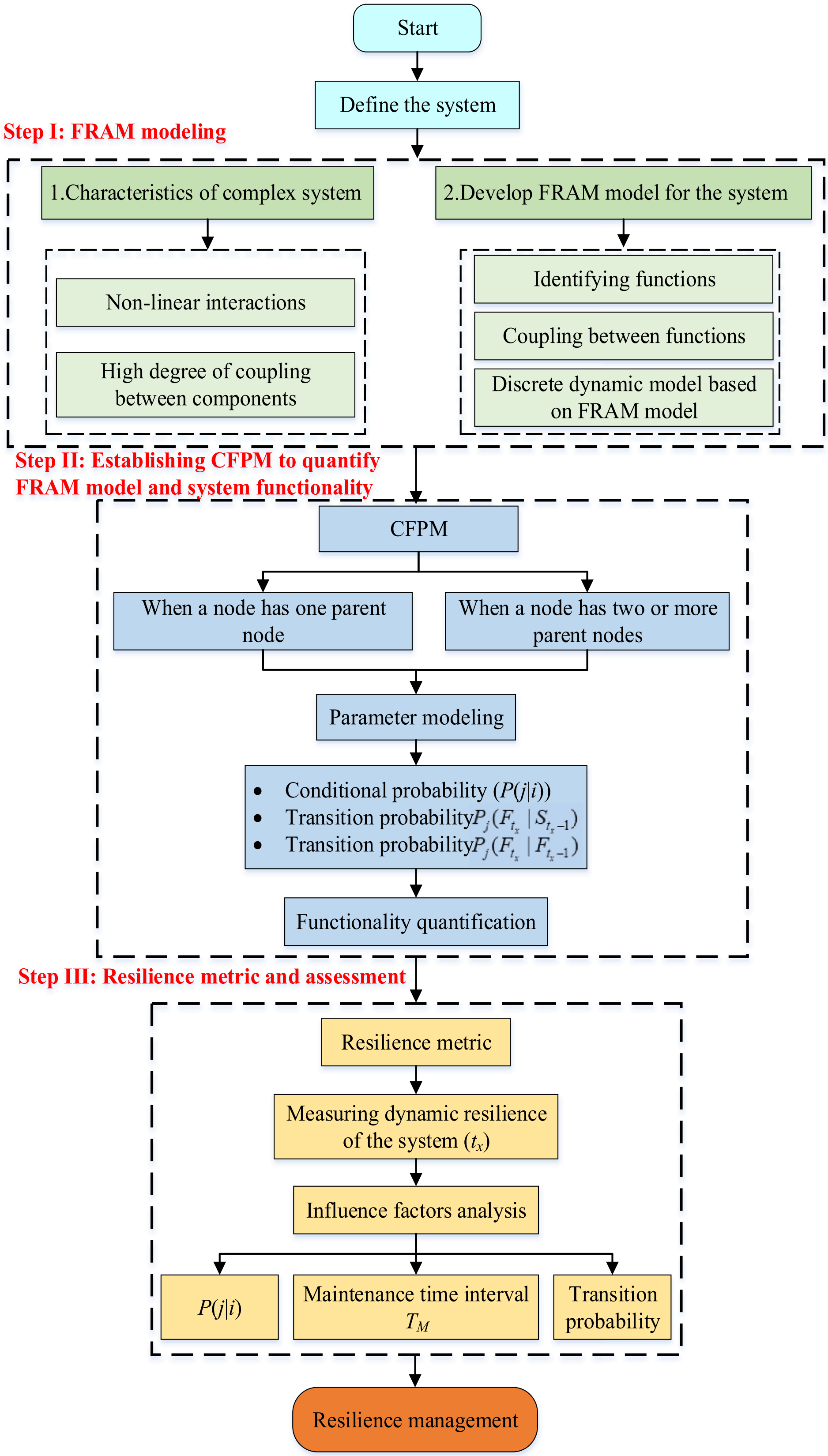
Start
Define the system
Step I: FRAM modeling
1.Characteristics of complex system
Non-linear interactions
High degree of coupling between components
2.Develop FRAM model for the system
Identifying functions
Coupling between functions
Discrete dynamic model based on FRAM model
Step II: Establishing CFPM to quantify FRAM model and system functionality
CFPM
When a node has one parent node
When a node has two or more parent nodes
Parameter modeling
Conditional probability ($P(j|i)$)
Transition probability$P_j(F_{t_x} | S_{t_x-1})$
Transition probability$P_j(F_{t_x} | F_{t_x-1})$
Functionality quantification
Step III: Resilience metric and assessment
Resilience metric
Measuring dynamic resilience of the system (t_x)
Influence factors analysis
$P(j|i)$
Maintenance time interval T_M
Transition probability
Resilience management

Fig. 1. The proposed methodology for assessing the system resilience.

technical, and organizational elements) have become large and less graspable risk factors in the process system. To be better prepared for the unforeseen and to deal with uncertainties, resilience thinking should be considered. The U.S. Department of Defense (DoD) (Neches, 2012) developed an engineering resilient system procedure, stating that the system should be able to resist/absorb disturbances, recuperate from disruptions, and adapt to changing conditions. Naghshbandi et al. [16] pointed out that uncertainty and interdependency significantly influence the resilience of a complex system. Any malfunction of one component or subsystem of a process system can affect other components and lead to a state fluctuation (i.e., "domino effect") in the system. To prevent and reduce performance and economic loss, it is essential to increase the resilience of the process system to cope with uncertain faults or disruptions [17]. Therefore, resilience is vital in ensuring system safety and mitigating functionality loss. Besides, resilience engineering (RE) is wider than RA since RE extends the traditional RA to the pre-and post-accident phases.

Resilience as a novel paradigm has attracted the attention of scholars [18–20]. Tong et al. [21] introduced an integrated method based on dynamic Bayesian network (DBN) to assess the system resilience according to absorption, adaption, and restoration ability. To measure system resilience, Yang et al. [22] developed a comprehensive approach, which comprised deterministic and probabilistic metrics. Jain et al. [23] developed a process resilience analysis framework (PRAF). Zinetullina et al. [24] presented a hybrid approach, which integrated Functional Resonance Analysis Method (FRAM) and DBN to quantify system resilience. Cincotta et al. [25] proposed a method that considers vulnerability and recoverability to raise the system resilience of firefighting strategies. Due to disturbance uncertainty, especially in the human-technical system, RE is an ideal method to reduce performance loss and enhance system safety. In light of different research domains, there is no uniform approach for assessing system resilience. The safety level of a system depends on its structure and function [26,27]. Almost all subsystems of a complex system have interacting components with different functions. Therefore, the basis of resilience assessment is defining the system boundaries, determining the optimal system performance, correctly analyzing the structure and internal functions of a system, and modeling it systematically. Although many current models for resilience evaluation in complex systems consider the system complexity and interdependencies, the comprehensive understanding of the interactions among equipment, human, and organization and their impact on system resilience is missing.

In light of many accident reports and investigations (HSE, 2011; [28–30]), when workers observed hazards or faults, to maintain the continuation of production (i.e., to reduce the economic loss caused by downtime), they are prone to deal with hazards online instead of shutting down the system for maintenance. Owing to the strong interdependencies and interactions between functions caused by a digitalized, automated, and complex system, the fault propagated to downstream nodes with some probability, which in the end, may bring about accidents. For instance, On August 6, 2012, a severe fire accident that resulted from a pipe rupture in the crude distillation unit happened at Richmond refinery in the USA. The accident steamed from the "4-side cut" leaving the Richmond refinery's C-1100 Crude unit atmospheric column [31]. When workers found the loss of containment and reported it, the managers decided to perform maintenance without utilizing the Stop Work Authority to ensure production continuation, which eventually led to the fire accident. Details of the Richmond refinery accident can be seen in the investigation report [28]. The accident reports prove that faults may propagate to downstream nodes even with online maintenance measures, and risk may build up over time until an accident occurs [32]. Already in the 1970s, Turner (1978) noticed this and called it the incubation period. Therefore, it is meaningful to conduct a resilience assessment to develop a more resilient system to prevent accidents and support decision-making.

In light of Safety-II, Functional Resonance Analysis Method (FRAM) is proposed as a systematic approach to analyzing human-technical system hazards and interactions between functions [33]. Compared with Safety–I, which pays more attention to reducing system failures and hazards, Safety–II believes that changes in the performance of system functions are inevitable and can lead to high-performance peaks but also failures. The system should be resilient and be able to deal with variability and uncertainty and adapt to changing conditions. FRAM has been proven to be an efficient method to reflect better the characteristics (i.e., interdependencies and interactions) of complex systems and model complex systems systematically. Due to the advantages of FRAM, it has been utilized in many research fields [34,35]. However, FRAM is a qualitative method making a system more transparent with respect to interactions and assesses system safety, but it cannot provide a dynamic resilience profile to support decision-making. To overcome this shortcoming, a quantitative approach is developed, including a novel cascading failure propagation model (CFPM), to measure system resilience. Cascading failure refers to a failure scenario in which a node failure, caused by internal or external disturbance, propagates to the downstream nodes and may lead to failure of the entire system.

The present study aims to develop a comprehensive approach comprising FRAM and a novel CFPM to measure resilience systemically. Firstly, FRAM is employed to model the system to reflect the complex and non-linear relationship between functions. After that, the FRAM model is converted into a discrete dynamic model to better represent the fault propagation when a fault occurs. Finally, CFPM is presented to describe the functionality variation process and measure the process of fault propagation and assess the resilience of an example process system under real-world engineering situations.

The remainder of this paper is organized as follows. A brief description of the proposed method, including the FRAM model, a novel CFPM model, and how to measure system resilience based on the FRAM and CFPM, is presented in Section 2. The case study is conducted in Section 3. Section 4 discusses the influence of different parameters for the CFPM on system functionality and resilience. Finally, Section 5 concludes this paper.

2. The proposed methodology

This section proposes the methodology to assess system resilience, which comprises three main parts: 1) modeling the system using the FRAM, 2) establishing the CFPM model to quantify the FRAM model and system functionality, and 3) measuring the system resilience. To begin with, FRAM analysis is carried out to identify interactions and couplings between functions. After that, the system is developed as a discrete dynamical system based on FRAM, which can be utilized to determine function states in different time-varying sequences. Then, the CFPM model, consisting of parametric modeling, is proposed to quantify the FRAM model to determine the system functionality curve. Finally, resilience metric is proposed to measure system resilience. The following section describes details of the main steps for the proposed method. The specific procedure is shown in Fig. 1.

2.1. Step I-FRAM modeling

In conventional safety assessment, systems are regarded as linear, which is decomposable and well-understood. The accident occurs because some components (e.g., human, organizational, and technical factors) in the system have problems. The main task of safety analysis is to find hazards and solve them, which belongs to "*causality credo*". In this idea, the function of a system is viewed as bimodal (i.e., function and malfunction) [27].

Nevertheless, technology is moving fast, making process systems more digitalized, automated, and complex. Unlike the previous liner system, the current process system in the chemical industry is a typical complex system with multiple functions and a complex hierarchical structure, which comprises information flow, material flow, and energy

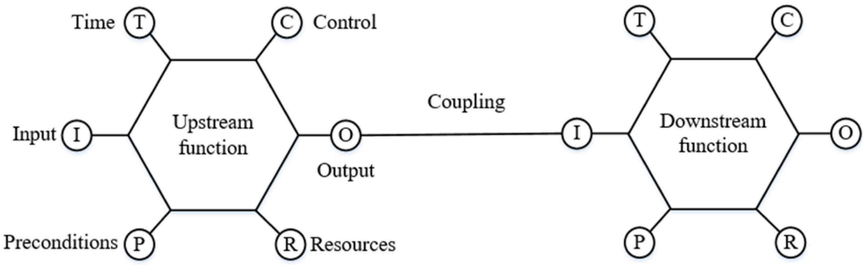

Fig. 2. Six aspects of FRAM function and the coupling between functions [33].

flow. The process system operation is always accompanied by hazardous factors (e.g., high temperature, pressure, poison, etc.), which may cause accidents and even disasters. Besides, the high degree of complexity caused by the non-linear interdependencies and interactions between functions leads to high variability and uncertainty. Therefore, the function of the system may not be seen as bimodal but dynamic and uncertain. The main task of safety should shift from discovering and solving hazards to coping with faults, disruptions, and system variabilities and maintaining the system in a safe state.

The conventional resilience assessment approaches cannot sufficiently identify and capture the interactions and coupling between functional aspects. The most successful approach to understanding complex relationships is FRAM. [33] developed FRAM with a particular context of organizational and psychological resilience engineering. The method quickly found many applications in accident analysis and others (Patriarca et al., 2020) and proved to be very suitable for understanding human-technical systems [36], which defines coupling between functions dynamically and promotes a systematic analysis of system function and state [37]. FRAM plays a pivotal role in resilience assessment, and it could be viewed as a feasible approach for two reasons:

(1) FRAM can recognize functional interdependencies and interactions for a complex system since it utilizes a bottom-up method from operational aspects to facilitate understanding process systems.
(2) FRAM characterizes a system by function instead of structure, which can better reflect resilience parameters by actions of components [27].

To assess system resilience, the first task is to identify how a system is functioning. The complexity and uncertainty of human-technical systems make it difficult to understand a system thoroughly. Therefore, a systematic method is vital for reflecting a complex system's details and functions. In this paper, the FRAM is used to characterize the interactions between system functions and better understand how a system is under control and maintained in a safe state when a disturbance occurs.

The FRAM follows four principles [33]. (1) A system goes wrong for the same reasons as it is successful. (2) The performance of a system is often adjusted following the changing environment. (3) The results of a system are emergent instead of resultant. (4) The variability of different functions produces resonance, which brings about abnormal function variability.

Before the FRAM analysis, the aim of the analysis should be determined first. In other words, it is essential to clarify whether the analysis aims to analyze accidents or to assess system risk [27]. After that, the FRAM analysis comprises four steps:

Step 1: Determining system functions;
Step 2: Describing variability of functions;
Step 3: Looking for functional resonance;
Step 4: Managing function variability.

Step 1, determining system functions is the basis for FRAM analysis. Both Leveson [38] and Hollnagel [33] tackled how to analyze human-technical systems. Leveson's STAMP (system-theoretic accident model and processes) is rigidly analyzing all control loops, which from the hierarchical top down to the bottom entails more and more details, while Hollnagel's approach is rather loose but requires more system understanding from the analyst. In his FRAM, each function is represented by a hexagonal module or node Fig. 2) with at the vertices the following aspects: ((1) Input (I): regarded as what is utilized or changed by the function; (2) Output (O): referring to the result of the function; (3) Preconditions, which must be met before conducting the function. For instance, one of the preconditions for a sensor is a good layout scheme; (4) Resources (R), which may constrain a function with regard to required availability (e.g., funds, manpower, and materials, etc.); (5) Control (C), which is supervising or adjusting a function to produce the desired output. (6) Time (T) restricting the function with respect to both length of action time and time of execution. Within the function node, no detail is modeled.

Functions are used to explain the actions of the system. FRAM model can be developed by defining the functions of which a system consists, identifying whether certain aspects are essential for the function in its interactions and interdependencies with other functions. In other words, the interactions and interdependencies among linked functions are viewed as upstream-downstream coupling, shown in its simplest form in Fig. 2.

In Step 2, FRAM analysis should focus on the variability of the output for the function rather than the variability of the function itself. Three ways can make output variables: endogenous variability, exogenous variability, and functional upstream-down-stream coupling. In light of Hollnagel [33], two methods are available to evaluate the variability of functions, i.e., a detailed approach and a simplified way . The detailed approach for variability assessment considers seven factors: time, duration, force, distance, direction, object, and sequence. The simplified method evaluates the variability of functions based on time and precision. The variability of function output often has the following two reasons: first, the change of the function or the change of the environment leads to the output variability; The second is the output change of the upstream function, which causes the downstream function to be affected. The variability of the upstream function mainly affects the action time and precision of the downstream function. Therefore, it is worth noting that this study assesses variability according to time and precision. These two phenotypes can be used to characterize most of the results. Besides, these phenotypes are universally applicable to any function [27]. In Step 3, by understanding the way the system operates safely, determining the way of coupling between functions, and explaining the typical variability of the functions, the reasons why the results of the system operation in a particular situation are different from many other smooth situations can be determined. The last step refers to managing the performance variability. Variability may result in positive or negative impacts. If the impact is positive, it should be expanded while ensuring the functionality of the system. On the contrary, the negative effects should be eliminated.

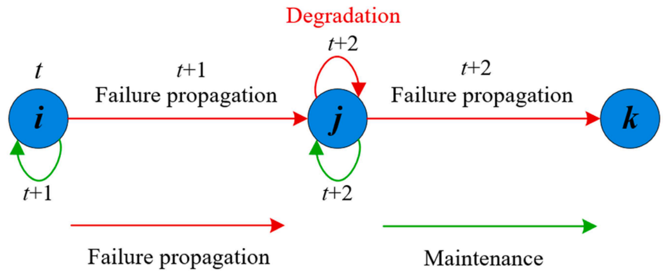

Fig. 3. The process of failure propagation on timeline.

2.2. *Step II-establishing CFPM to quantify the FRAM model and measure system functionality*

FRAM, as discussed above, is an efficient model to develop and reflect the complex interactions and interdependencies among functions. The functionality change of a node in the system will cause functionality change in downstream nodes, which is called fault propagation. There are two tasks to conduct when measuring a system resilience using FRAM: (1) FRAM addresses the spatial interdependencies and interactions of functions and thus models the system operation; (2) When the function of a component fails in a process system, it will affect the function of downstream nodes with a certain probability in the next time interval. The output (i.e., O) of a function for an upstream component always influences one or more aspects (i.e., T, C, I, P, R) of downstream components to a certain degree [39]. Thus, we convert the FRAM into a discrete dynamical system (i.e., a directed model) to determine function states in different time-varying sequences.

Before major accidents occur, there is usually a period of time of precursor occurrences during which the system gradually moves toward a state of increased risk until an event occurs that leads to losses [32]. Risk accumulation is the result of process of fault propagation. Quantifying and understanding this process is of great significance for ensuring system safety. To measure the process and explain the mechanism of fault propagation, a novel CFPM model is developed. It can be used to describe in detail the functionality of each node at different times during the process of fault propagation to help practitioners better understand the changes in system functionality over time. Moreover, it can be utilized to quantify the fault propagation process and determine the system functionality changes over time, which can be employed to measure the system resilience.

A novel CFPM is then established to quantify the temporal interdependencies and interactions of functions according to the FRAM.

This subsection proposes a new CFPM to quantify the process of fault propagation and measure system functionality. As discussed earlier, even if the system's functional problems are observed, operators tend to maintain the system online instead of using Stop Work Authority (i.e., shutting down the unit) [28].

When a node is affected by a disturbance, it will cause the performance and functionality of the node to degrade or malfunction. The changes in the node's state will influence its downstream nodes [40]. Therefore, the FRAM is converted into a discrete dynamical system, which can be utilized to identify a series of time-varying sequences of system state [41]. For example, node *I* is malfunctioning at time *t*, and at the next time increment (i.e., *t*+1), the fault will spread to node *j*, while node *i* will recover with a particular probability. The rest can be calculated in the same manner. The process for failure propagation is shown in Fig. 4. Note that the red line indicates the process of failure propagation, and the green line represents the effect of the maintenance process (Fig. 3).

If an operator decides to maintain the malfunctioned nodes, those nodes will recover their lost functionality gradually. The failure probability of node *j* at time *t*+1 is shown as Eq. (1), and the failure probability of node *j* at time *t*+2 can be described as Eq. (2).

$$P_j(t+1) = P_i(t) \times P(j|i) \tag{1}$$

$$P_j(t+2) = P_j(t+1) \times P_j(F_{t+2}|F_{t+1}) + \left[1 - P_j(t+1)\right] \times P_j(F_{t+2}|S_{t+1}) \tag{2}$$

where $P_i(t)$ is the failure probability of node *i* at time *t; P*($j|i$) indicates propagation probability of node *i* malfunction causes node *j* fails; $P_j(F_{t+2}|F_{t+1})$is transition probability and stands for the failure probability of node *j* at time *t*+2 when node *j* fails at time *t*+1; $P_j(F_{t+2}|S_{t+1})$ is transition probability and stands for the failure probability of node *j* at time *t*+2 when node *j* successes at time *t*+1; It is worth noting that if a node has no upstream node, it is only affected by itself.

It is worth noting that $P_j(t+2)$ may be less than 0 in Eq. (2). Thus, when $P_j(t+2)$ is equal to 0, node *j* can be viewed as a normal node in a safe state, and its failure probability is 0.

When node *j* is affected by node *i* at time t_x ($t_x \geq 2$), its failure probability can be described as Eq. (3):

$$P_j(t_x) = P_j(t_x - 1) \times P_j(F_{t_x}|F_{t_x-1}) + \left[1 - P_j(t_x - 1)\right] \times P_j(F_{t_x}|S_{t_x-1}) \tag{3}$$

When node *j* is jointly affected by two or more independent nodes, its failure probability can be expressed as Eq. (4). This means that as long as one of those upstream nodes of node *j* fails, the state of node *j* will be affected.

$$\begin{aligned} P_j(t_x) = P_j(F_{t_x}|F_{t_x-1}) + \prod_{u=1}^{n}(1 - P_u(t_x - 1) \times P(j|u)) \\ \times \left[P_j(F_{t_x}|S_{t_x-1}) - P_j(F_{t_x}|F_{t_x-1})\right] \end{aligned} \tag{4}$$

where *u* indicates a node that affected node *j*, *n* represents the number of nodes that affected node *j*. Node *j* can be viewed as a malfunctioning node when$P_j(t_x) \ = 1$.

On the contrary, the state of node *j* changes only when two or more upstream nodes fail at the same time. This is similar to the AND gate in the fault tree. In this situation, Eq. (4) can be converted to Eq. (5):

$$\begin{aligned} P_j(t_x) = P_j(F_{t_x}|S_{t_x-1}) + \left[\prod_{u=1}^{n}(P_u(t_x - 1) \times P(j|u))\right] \\ \times \left[P_j(F_{t_x}|F_{t_x-1}) - P_j(F_{t_x}|S_{t_x-1})\right] \end{aligned} \tag{5}$$

The states of each node can be determined by Eqs. (3), (4) and (5). Therefore, the functionality for a system (i.e., the whole network that was developed based on FRAM) can be measured by those node state at time sequence, which can be represented by Eq. (6).

$$F_S\left(t\right) = 1 - \frac{\sum_{a=1}^{m} f_a \cdot P_a(t)}{\sum_{a=1}^{m} f_a} \tag{6}$$

where F_s represents the functionality of the system, *m* indicates the total number of nodes in the system, *t* means the discrete time, which satisfies $0 \leq t \leq t_f$, t_f is the failure time of the system, f_a shows weight of node *a*, which is expressed in Eq. (7).

$$f_a = \frac{d_a}{m} \tag{7}$$

where d_a indicates the number of nodes connected to node *a, m* represents the number of nodes in the system. Note that the more important the node, the greater the impact of its state on the system.

2.3. *Step III-resilience metric and assessment*

Once the functionality curve is obtained, the system resilience can be represented as a dimensionless ratio [42]. Resilience should be regarded as the proportion of functionality restored through maintenance actions. In the light of the resilience framework proposed by Bruneau et al. [42],

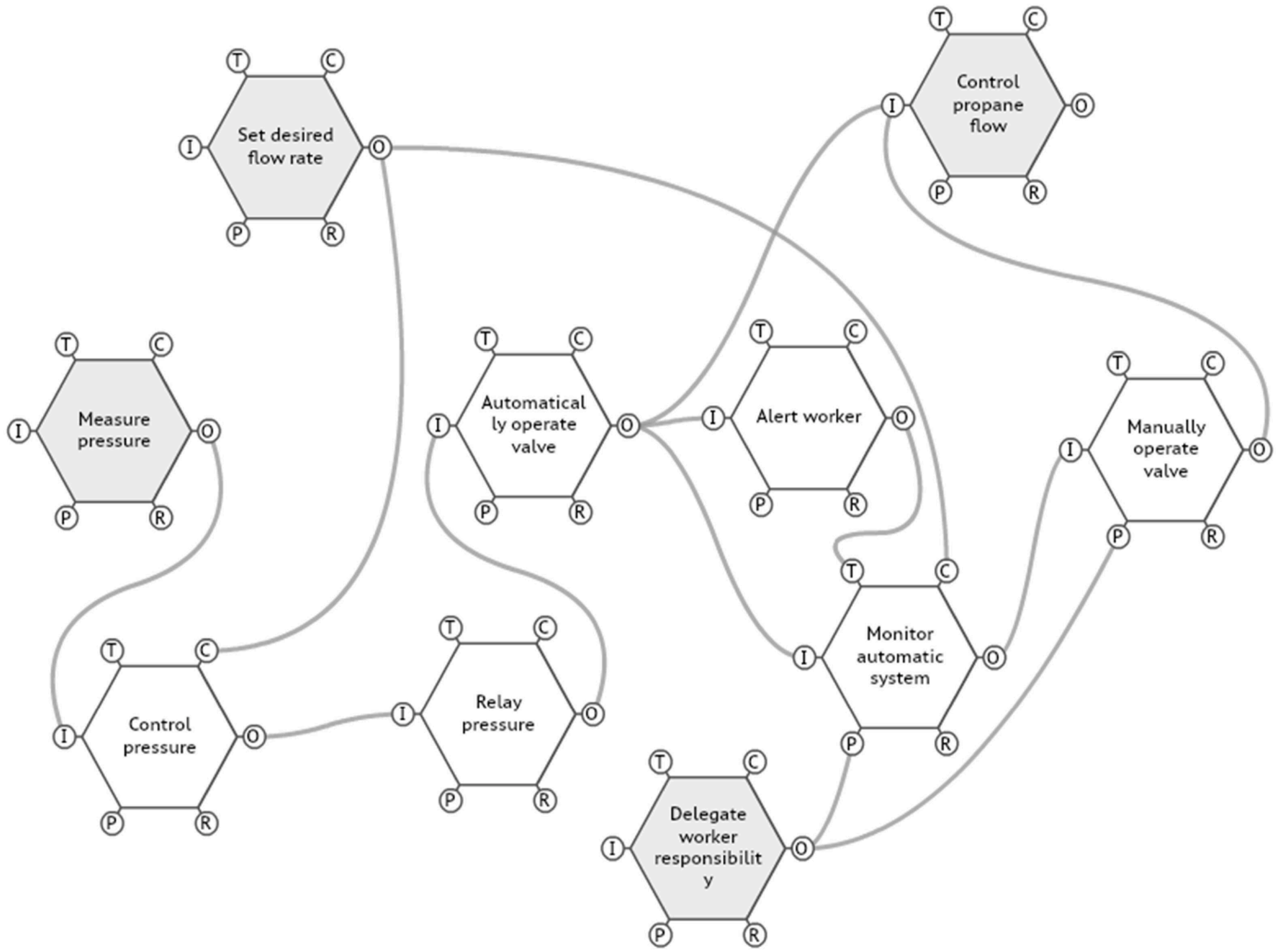

Fig. 4. The FRAM model for the propane feeding system (adapted from [46]).

resilience can be expressed as Eq. (8).

$$\text{Я}\left(t\middle|e^j\right) = \frac{\varphi\left(t\middle|e^l\right) - \varphi\left(t_d\middle|e^l\right)}{\varphi(t_0) - \varphi\left(t_d\middle|e^l\right)} \tag{8}$$

where$\text{Я}\left(t\middle|e^j\right)$indicates system resilience at time t; $\varphi\left(t\middle|e^l\right)$represents system functionality at time t; $\varphi\left(t_d\middle|e^l\right)$ is the lowest functionality of the system; $\varphi(t_0)$ indicates the initial functionality of the system before the occurrence of the fault. Eq. (8) can be changed to Eq. (9) by integrating the Eq. (6) on the time term.

$$\text{Я}(S) = \frac{\int_{t_0}^{t_x} F_S(t)dt}{R(t_0)(t_x - t_0)} \tag{9}$$

where$\text{Я}(S)$indicates the system resilience; $R(t_0)$ represents the initial functionality of the system before the occurrence of disturbance; t_x represents the time ($t_x > t_0$); t_0 is the time that the disturbance occurs.

However, when the types of functionality curve are different,$\text{Я}(S)$ may give a same value of resilience for different combinations of $F_S(t)$ and t_x [43]. To solve the limitation of resilience metric,$\text{Я}(S)$, Sharma et al. [44] proposed Center of Resilience and Resilience Bandwidth based on probability theory and mechanics. The recovery curve $Q(\tau)$ is defined as *Cumulative Resilience Function* (CRF). When the CRF is a continuous function of time, the Instantaneous Rate of the Recovery Progress (IRRP) can be obtained by the time derivative of the CRF. IRRP is regarded as $q(\tau)=dQ/d\tau$ for all $\tau\in[0, T_R]$, which is called *Resilience Density Function* (RDF). T_R indicates the whole recovery time. Then, the recovery process over any time interval $(\tau_u, \tau_v] \subseteq [0, T_R]$ is shown in Eq. (10). When the CRF is a step function or a combination of continuous function and step function of time, the recovery process over any time interval can be seen in Sharma et al. [43]

$$Q(\tau_u < \tau < \tau_v) = \int_{\tau_u}^{\tau_v} q(\tau)d\tau \tag{10}$$

The Center of Resilience ρ_Q, which combines residual functionality and recovery time, is defined as:

$$\rho_Q := \frac{\int_0^{T_R} \tau q(\tau)d\tau}{\int_0^{T_R} q(\tau)d\tau} = \frac{Q_{res}}{Q_{tar}}\rho_{Q,res} + \frac{Q_{res1}}{Q_{tar}}\rho_{Q,res1} \tag{11}$$

where Q_{res} represents the residual functionality of system, Q_{tar} equals to $Q(T_R)$, $\rho_{Q,res}=\tau_0$, $Q_{res1}= Q_{tar}$ - Q_{res}. Due to $\tau_0=0$, Eq. (11) can be converted into Eq. (12).

$$\rho_Q = \frac{Q_{res1}}{Q_{tar}}\rho_{Q,res1} \tag{12}$$

The Resilience Bandwidth χ_Q, as a measure of dispersion of recovery, is defined as:

$$\chi_Q^2 := \frac{\int_0^{T_R} (\tau - \rho_Q)^2 q(\tau)d\tau}{\int_0^{T_R} q(\tau)d\tau} \tag{13}$$

The small χ_Q means that the recovery process is finished during a short period around ρ_Q. On the contrary, the large one indicates that the recovery process is spread in a long time. Once the system functionality

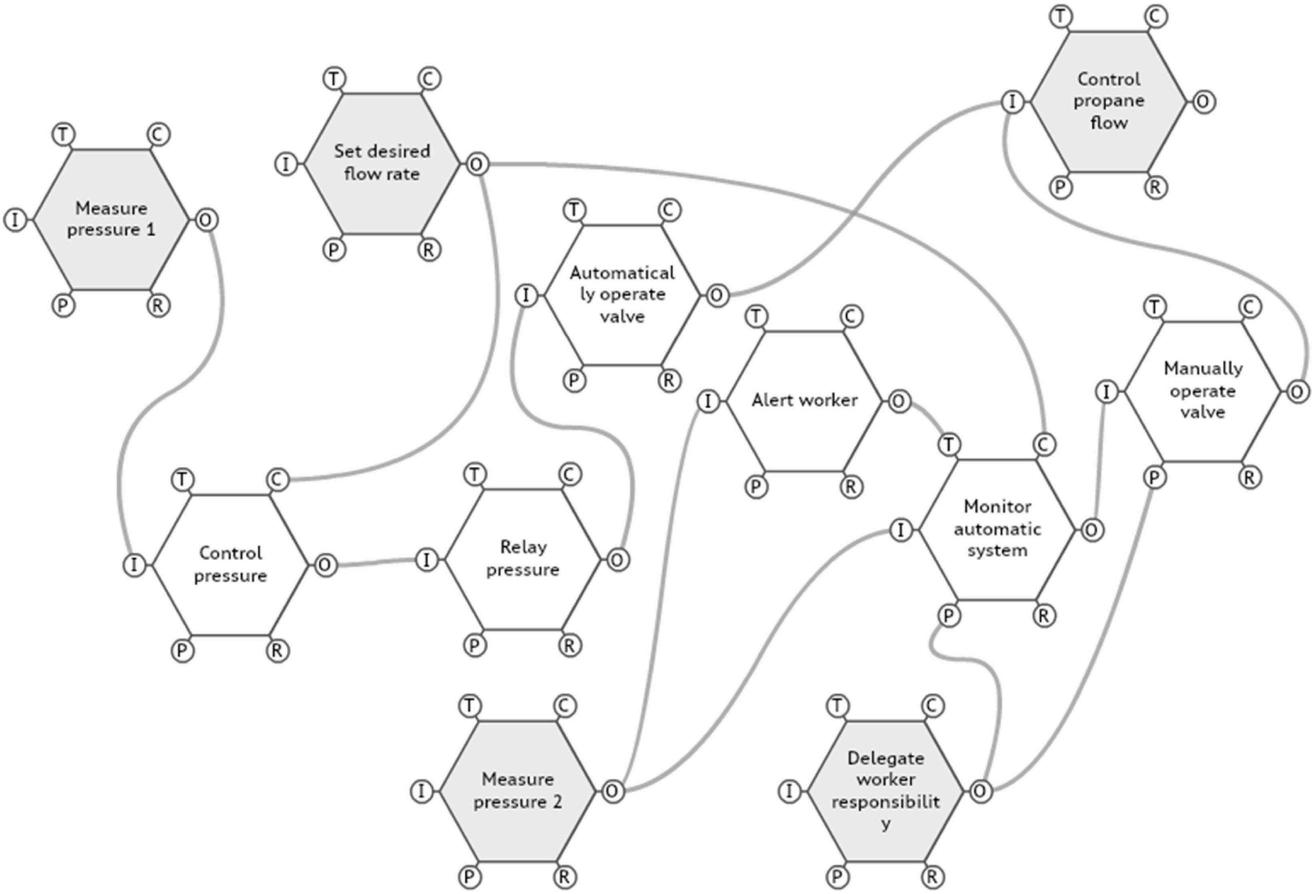

Fig. 5. The improved FRAM model for the propane feeding system (adapted from [46]).

curve is obtained, the ρ_Q and χ_Q can be determined based on Eqs. (12) and (13).

3. Case study

3.1. FRAM modeling and its conversion

(1) The FRAM model for a propane feeding control system

A propane feeding control system, which comprises an automatic and manual control system, is selected to demonstrate the proposed method. The key tasks of establishing FRAM model are identifying functions and developing coupling relationship between functions.

The main control sequence of the propane feeding control system is as follows: 1) By setting the desired flow rate and measuring the system pressure to maintain the system pressure under control; 2) When the pressure exceeds the threshold, the automatic operating valve should be opened automatically and send the alarm to workers; 3) At the same time, the propane flow rate should be adjusted, and the automated system should be monitored; 4) If the automatic operating valve malfunctions, the workers should open the manual valve to release pressure to keep the system safe [45]. According to the control sequence of the system, the function of each step and their coupling relationships can be determined. The FRAM model for the system has been modeled by Smith et al. [46], shown in Fig. 4.

Owing to the importance of the pressure in the system, Smith et al. [46] suggested improving the system by adding another sensor to measure the system pressure. The FRAM model of the improved system is shown in Fig. 5. In the enhanced system, if sensor 1 (i.e., Measuring pressure 1 in Fig. 5) malfunctions, the automatic operating valve cannot be activated because the wrong detected pressure might not be greater than the pressure threshold. This may lead to an accident when the pressure exceeds the threshold since the pressure sensor fails to detect and report it. Due to the existence of sensor 2 (i.e., Measuring pressure 2 in Fig. 5), even if sensor 1 fails to measure the system pressure correctly, sensor 2 plays a vital role in detecting the pressure and alerting the workers. When the workers are notified by sensor 2, they will monitor the system pressure and open the manually operating valve when the pressure surpasses the safe threshold.

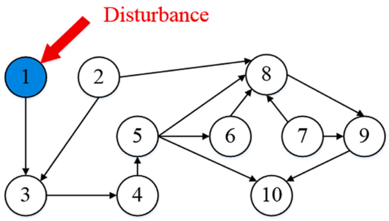

Fig. 6. The discrete dynamic model extracted from the FRAM model for the original propane feeding system.

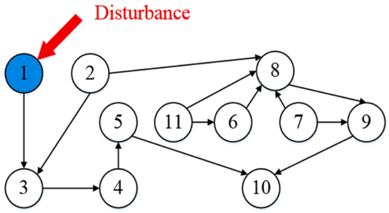

Fig. 7. The discrete dynamic model extracted from FRAM model for the improved propane feeding system.

Table 1
The descriptions of each node in the FRAM model and discrete dynamic model.

Node	Description
1	Measure pressure 1
2	Set the desired flow rate
3	Control pressure
4	Relay pressure
5	Automatically operate valve
6	Alert worker
7	Delegate worker responsibility
8	Monitor automatic system
9	Manually operate valve
10	Control propane flow
11	Measure pressure 2

Table 2
The weight of each node in two different systems.

	The original system	The improved system
Node	d_a	d_a
1	1	1
2	2	2
3	3	3
4	2	2
5	4	2
6	2	2
7	2	2
8	5	5
9	3	3
10	2	2
11	–	2

(2) The discrete dynamic model converted from FRAM mode

As discussed earlier, the output of a function for an upstream node always impacts one or more aspects of downstream nodes to a certain degree [39]. In other words, if a disturbance occurs at an upstream node, it will affect the functionality of this node, and the fault will propagate to the downstream node with a particular probability. Therefore, to assess the system resilience, the FRAM is converted into a discrete dynamical model, which can be used to determine a series of time-varying sequences of system states. The discrete dynamic models converted from Figs. 4 and 5 can be seen in Figs. 6 and 7. The descriptions of each node are shown in Table 1. It is worth noting that this paper assumes that the disturbance occurs on node 1. After that, the proposed CFPM is used to describe this kind of propagation process, and a resilience metric is proposed to measure the resilience of the system and the improved system safety, which is specifically described in the next subsection.

3.2. *Quantification of the system resilience*

According to the FRAM model and discrete dynamic model developed in Section 3.1 (i.e., Figs. 6 and 7), the relationship between each node can be determined, which means that when the upstream node malfunctions, it will cause functionality change of the downstream node. The specific influence of propagation probability is discussed in Section 4.

The proposed CFPM is utilized to quantify system functionality during the process of fault propagation. Duo to the interaction and interdependence between system nodes, when a node is affected by disruptions, the state of downstream nodes will be impacted by the affected node. According to state and weight of each node, the system dynamic functionality can be determined based on the CFPM model. In the light of Eq. (7), Figs. 6, and 7, the weight d_a of each node can be determined and shown in Table 2.

According to Eqs. (1), (3), (4), and (5), the states of each node in different time sequences can be quantified. Once the state of each node of the system is obtained, Eq. (6) is then employed to quantify the state of the system at a different time (40 time intervals are used to demonstrate the proposed approach), which can help determine the functionality curves, as shown in Fig. 8. Finally, Eq. (9) is utilized to assess dynamic resilience of the system, and the results can be seen in Fig. 9. The black line indicates the original system, and the red line represents the improved system.

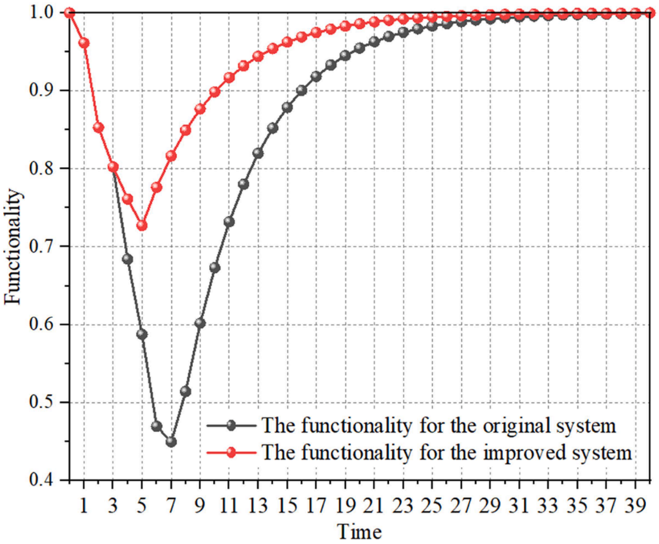

Fig. 8. The functionality curve for two different systems.

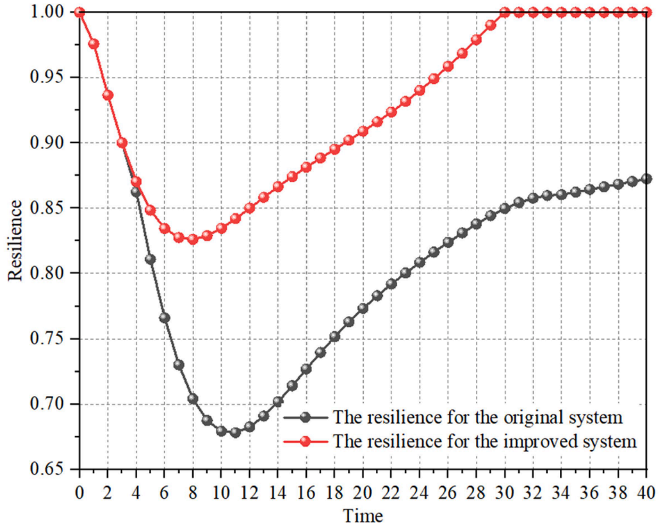

Fig. 9. The resilience of two different systems.

Maintenance measures can mitigate the speed and degree of fault propagation. However, repair activity is a process and requires resources (e.g., time, money, manpower, etc.) to conduct. It can be seen from Fig. 8 that the system functionality decreases first, which is caused by fault propagation. For the original system, the minimal functionality is 0.45 at time t+7. After this, with the repair activity, the functionality for each node recovered gradually, and the functionality of the system increases over time. For the improved system, the minimal functionality is 0.73 at time t+5, which means that the improved system has a greater absorption capacity to deal with the same disruption events.

For the original system, the fault is propagated to downstream nodes from node 1 at time t, leading to the resilience decrease. Then, the system resilience dropped to the minimum value (0.678) at time t+11. After that, the effect of maintenance activities is gradually showing up, and the state of nodes in the system begins to recover, results in an

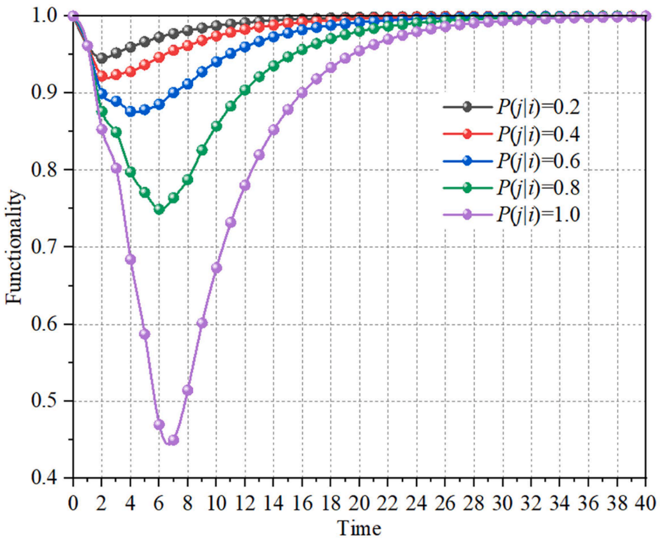

Fig. 10. The system functionality changes with different $P(j|i)$.

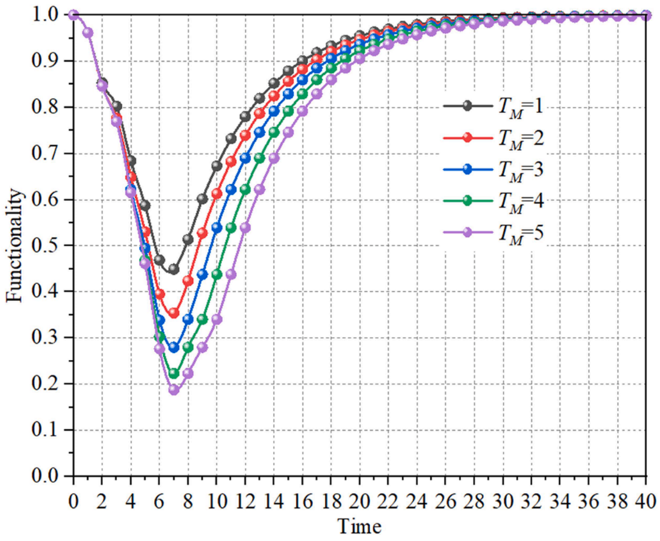

Fig. 11. The system functionality changes with different maintenance time.

increase in the system resilience. The speed and degree of recovery for nodes depend on $P_j(F_{t_x}|F_{t_x-1})$. For the improved system, the fault is spread to downstream nodes from node 1 at time t, leading to the resilience reduce, which is same as the original system. After that, the system resilience reduced to the least value (0.826) at time t+8. What followed is that the resilience of the system began to increase gradually. Comparing the two (i.e., the original system and the improved system) can be found that the resilience of the improved system is stronger than that of the original system, which is mainly reflected in two aspects. The first one is the absorption ability is different. The improved system has a stronger absorptive capacity resulting from the added sensors 2. When sensors 1 is affected by the disturbance, sensors 2 can measure the system pressure and inform the worker to open the manual pressure valve to ensure the system safety, which is why the minimum value of resilience for the improved system (0.826) is bigger than that of the original system (0.678). The second one is the capacity for adaptation and restoration. The improved system possesses higher adaptation and restoration ability. It can be seen from Figs. 6 and 7, when the disturbance occurs at node 1, the fault will propagate to downstream nodes (i.e., node 3, 4, 5, 6, 8, 9, and 10) in the original system, while the fault will spread to node 3, 4, 5, and 10 in the improved system. The enhanced system cuts off the connection between node 5 and node 6, and node 8, which means that the interdependence between them is reduced. As a result, the number of affected nodes is reduced so that resources can be concentrated to repair fewer affected nodes. This is why the resilience of the improved system starts to increase earlier than that of the original system. The specific information can be seen in Fig. 9.

By comparing the resilience of the original system and the improved system, it can be seen that changing system structure (e.g., set up backup equipment) is a potential method to improve system resilience. The interdependence between components or nodes will affect the degree of fault propagation and the states of each node, thereby affecting the system resilience. By optimizing the system, especially by reducing the interdependence between nodes, the resilience of the system can be significantly enhanced. Therefore, the safety and resilience of a complex system can be improved from some aspects: i) increasing the maintenance efficiency and ii) optimizing the system (e.g., adding a standby sensor in this case). Other ways to improve system resilience will be discussed in detail in the next section. The engineering meaning of the proposed approach is to provide a dynamic resilience profile. Besides, it can help practitioners design and optimize a more resilient system to withstand uncertain disturbances (e.g., cyber-attack, internal and external attacks) to ensure system safety.

4. Discussions

4.1. The influence of model parameters on the system functionality and resilience

(1) The influence of conditional probability ($P(j|i)$)

The original system is used to demonstrate the influence of conditional probability (i.e., $P(j|i)$) on system resilience. The conditional probability $P(j|i)$ can be determined by expert judgements based on the specific system (e.g., the degree of interdependence among nodes) when practitioners utilize the proposed methodology. Without loss of generality, several values are used to study the influence of propagation probability on system resilience. The results are shown in Fig. 10.

It can be seen from Fig. 10, with the increase of the conditional probability $P(j|i)$, the system functionality decreases, which means that by reducing $P(j|i)$ the system resilience can be improved. When the fault occurs at node i, the fault will propagate to the downstream nodes (e.g., j) with the probability of $P(j|i)$. The smaller the $P(j|i)$, the more resilient the system is. In other words, the smaller the P($j|i$), the stronger the absorption capacity of the component is.

(1) The influence of maintenance time interval (T_M) and transition probability$P_j(F_{t+2}|F_{t+1})$

T_0 is defined as the time when the fault occurs at a node for the system. T_M represents the time interval from when the fault occurs at a node of the system to the maintenance activity starts. In this case, the time interval (i.e., T_M) 1 is used to illustrate the proposed approach. Besides, other three values of time interval are utilized to study the influence of time interval on system functionality, which are shown in Fig. 11. Maintenance time interval refers to whether the maintenance is timely. Fig. 11 shows that the smaller the time interval, the more resilient the system is. The system resilience can be raised by decreasing the T_M. In a real-world situation, this can be achieved by formulating relevant inspection policies and finding faults, and repairing them on time.

The transition probability is determined by the repair rate. The more maintenance resources, the higher the repair rate, which can reduce the value of $P_j(F_{t+2}|F_{t+1})$ and improve system functionality and resilience. The recovery process of this kind of interdependent system will rely on how maintenance resources are used. Under the circumstance that the available maintenance resources are fixed, the more important the node,

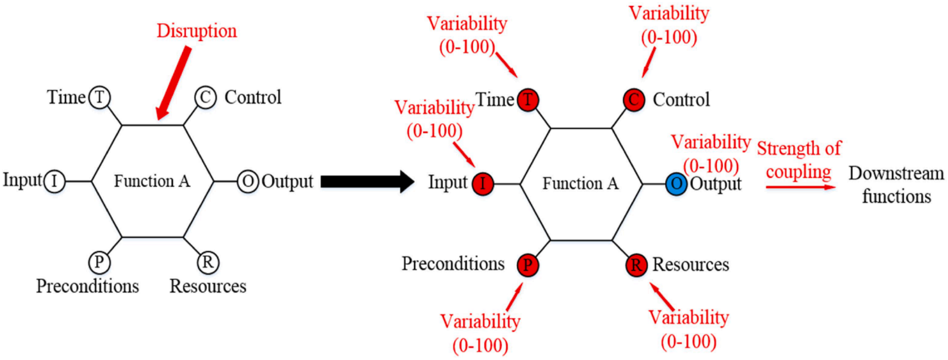

Fig. 12. The variability of five aspects affects output variability.

the more maintenance resources should be allocated. If the use of maintenance resources is random, then it may cause more physical and economic losses.

4.2. Limitation and scope for future study

FRAM is a systemic model that considers and represents an essential characteristic of a complex system, i.e., interdependencies and interactions between technological, human, and organizational factors. Resilience is a system's capacity to combat disruptions. Thus, resilience assessment should be conducted on the basis of a systemic model. This study employs FRAM to model the functional interdependencies and interactions of a complex system.

The proposed methodology has some limitations. In this study, FRAM is only utilized to identify the functional dependency of a system. The strength of function couplings measured by the FRAM model is not considered in the CFPM for quantitative resilience assessment. The propagation probability (i.e., $P(j|i)$) is regarded as a conditional probability similar to those used in a Bayesian network (BN). The greater the failure probability of the upstream node, the greater the degree of impact on the downstream node. Without loss of generality, the propagation probability $P(j|i)$ is set as 0.8 for illustrative purpose.

This study focuses on quantifying system resilience by considering non-linear interdependencies among human-technical factors. To further improve the proposed method, future work can be devoted to investigating how to incorporate the strength of function couplings in assessing system resilience. FRAM measures the variability of the Output rather than the function itself. The Output of a function is affected by five aspects: Time, Control, Input, Precondition, and Resource. Each aspect has different degrees of influence on the Output, which can be determined by its weight. When a disruption occurs at one function, variability may occur at one or more of these five aspects. The degree of variability can be described by a range of values, which is shown in Fig. 12. The variability of Output can be regarded as the state of the function, and the strength of function couplings can be viewed as the propagation probability. In this way, the system resilience could be measured based on these two steps. This work is in progress.

5. Conclusions

The rapid development of technology has made process systems complex, leading to strong interaction and interdependence between components. This brings two problems: (i) it is difficult for conventional methods to model the complex system. In other words, there is an urgent need for a method that can systematically model the system to accurately reflect the interdependency among the technical, human, and organizational factors; (ii) as the interaction and interdependency between functions is getting closer and robust, once a function is affected by a disturbance, it will influence other functions. Besides, there are two characteristics of disturbance in the digital age, i.e., diversity (e.g., cyber-attack, internal or external attack, intentional attack, etc.) and uncertainty (i.e., where, when, and how will it occur). Therefore, there is a need to take resilience thinking into account to make the system more resilient to deal with uncertain disturbances since building a resilient system is preferable to analyzing the system risk. This paper creates a comprehensive approach to solving these two problems. To analyze the interaction and interdependency between functions, the FRAM model is utilized and then converted to a discrete dynamic model to reflect the influence relationship between functions. Considering fault propagation, a novel CFPM model is proposed to analyze the fault propagation process and functionality curve. On that basis, an approach to measure system resilience is developed, which is able to provide a real-time resilience profile.

The case study shows that there are four ways to enhance the system resilience. The first one is optimizing the system to improve the absorption capacity, which can be proven by Fig. 9. Secondly, the system resilience can be improved by decreasing the conditional probability $P(j|i)$ between nodes. Thirdly, the resilience of the system can be boosted by reducing T_M, that is, taking inspection and maintenance measures timely. Lastly, strengthening and optimizing the maintenance resources can enhance the system resilience. The main contribution of the proposed approach is to help practitioners comprehensively improve the system resilience from different aspects to resist diversified and uncertain disturbances.

CRediT authorship contribution statement

Hao Sun: Conceptualization, Methodology, Formal analysis, Investigation, Writing – original draft, Writing – review & editing. **Ming Yang:** Conceptualization, Methodology, Formal analysis, Writing – review & editing, Validation. **Haiqing Wang:** Supervision, Writing – review & editing, Funding acquisition.

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.

Data availability

No data was used for the research described in the article.

Acknowledgments

The authors gratefully acknowledge the financial support provided by the Central Universities Fundamental Research Funds Project (YCX2021077) and China Scholarship Council under grant 202106450059.

References

[1] Abbassi R, Khan F, Garaniya V, Chai S, Chin C, Hossain K. An integrated method for human error probability assessment during the maintenance of offshore facilities. Process Saf Environ Prot 2015;94:172–9.

[2] Benson C, Argyropoulos CD, Dimopoulos C, Mikellidou CV, Boustras G. Safety and risk analysis in digitalized process operations warning of possible deviating conditions in the process environment. Process Saf Environ Prot 2021;149:750–7.

[3] Khan F, Wang H, Yang M. Application of loss functions in process economic risk assessment. Chem Eng Res Des 2016;111:371–86. Process. Saf. Environ. Prot. 135, 70–80.

[4] Mishra KB, Wehrstedt KD, Krebs H. Amuay refinery disaster: the aftermaths and challenges ahead. Fuel Process Technol 2014;119:198–203.

[5] Khan B, Khan F, Veitch B. A dynamic Bayesian network model for ship-ice collision risk in the arctic waters. Saf Sci 2020;130:104858.

[6] Misuri A, Landucci G, Cozzani V. Assessment of risk modification due to safety barrier performance degradation in Natech events. Reliab Eng Syst Saf 2021;212: 107634.

[7] Landucci G, Argenti F, Cozzani V, Reniers G. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf Environ Prot 2017;110:102–14.

[8] Sultana S, Anderson B, Haugen S. Identifying safety indicators for safety performance measurement using a system engineering approach. Process. Saf. Environ. Prot. 2019;128:107–20.

[9] O'Connor M, Pasman HJ, Rogers WJ. Sam Mannan's safety triad, a framework for risk assessment. Process. Saf. Environ. Prot. 2019;129:202–9.

[10] Zhu TT, Haugen S, Liu YL, Yang X. A value of prediction model to estimate optimal response time to threats for accident prevention. Reliab Eng Syst Saf 2023;232: 109044.

[11] Ghosh A, Ahmed S, Khan F, Rusli R. Process safety assessment considering multivariate non-linear dependence among process variables. Process Saf Environ Prot 2020;135:70–80.

[12] Mamudu A, Khan F, Zendehboudi S, Adedigba S. Dynamic risk modeling of complex hydrocarbon production systems. Process Saf Environ Prot 2021;151: 71–84.

[13] Zarei E, Azadeh A, Khakzad N, Aliabadi MM, Mohammadfam I. Dynamic safety assessment of natural gas stations using Bayesian network. J Hazard Mater 2017; 321:830–40.

[14] Sun H, Wang H, Yang M, Reniers G. On the application of the window of opportunity and complex network to risk analysis of process plants operations during a pandemic. J. Loss Prev. Process. Ind. 2020;68:104322.

[15] Chen C, Yang M, Reniers G. A dynamic stochastic methodology for quantifying HAZMAT storage resilience. Reliab Eng Syst Saf 2021;215:107909.

[16] Naghshbandi SN, Varga L, Purvis A, Mcwilliam R, Minisci E, Vasile M, et al. A review of methods to study resilience of complex engineering and engineered systems. IEEE Access 2020;8:87775–99.

[17] Pawar B, Park S, Hu PF, Wang QS. Applications of resilience engineering principles in different fields with a focus on industrial systems: a literature review. J. Loss Prev. Process. Ind. 2021;69:104366.

[18] Hosseini S, Barker K, Ramirez-Marquez JE. A review of definitions and measures of system resilience. Reliab Eng Syst Saf 2016;145:47–61.

[19] Jamaluddin K, Alwi S, Manan Z, Hamzah K, Klemes J. Hybrid power systems design considering safety and resilience. Process Saf Environ Prot 2018;120: 256–67.

[20] Pramoth R, Sudha S, Kalaiselvam S. Resilience-based integrated process system hazard analysis (ripsha) approach: application to a chemical storage area in an edible oil refinery. Process Saf. Environ. Protect. 2020;141:246–58.

[21] Tong Q, Yang M, Zinetullina A. A dynamic bayesian network-based approach to resilience assessment of engineering systems. J Loss Prev Process Ind 2020;65: 104152.

[22] Yang BF, Zhang L, Zhang B, Wang WF, Zhang ML. Resilience metric of equipment system: theory, measurement and sensitivity analysis. Reliab Eng Syst Saf 2021; 215:107889.

[23] Jain P, Pasman HJ, Waldram S, Pistikopoulos EN, Mannan MS. Process resilience analysis framework (PRAF): a systems approach for improved risk and safety management. J. Loss Prev Proc Ind 2018;53:61–73.

[24] Zinetullina A, Yang M, Khakzad N, Golman B, Li XH. Quantitative resilience assessment of chemical process systems using functional resonance analysis method and dynamic Bayesian network. Reliab Eng Syst Saf 2021;205:107232.

[25] Cincotta S, Kahkzad N, Cozzani V, Reniers G. Resilience-based optimal firefighting to prevent domino effects in process plants. J Loss Prev Process Ind 2019;58:82–9.

[26] Fogliatto FS, Ribeiro JLD. Confiabilidade e manutenc¸ ão industrial. São Paulo: Elsevier Editora; 2009.

[27] Patriarca R, Di Gravio G, Costantino F. A Monte Carlo evolution of the functional resonance analysis method (FRAM) to assess performance variability in complex systems. Saf Sci 2017;91:49–60.

[28] CSB. Chevron richmond refinery pipe rupture and fire California 2014. CA, August 6, 2012, http://www.csb.gov/. last checked 17.11.14.

[29] Liu ZH, Zhou JF, Reniers G. Association analysis of accident factors in petrochemical storage tank farms. J Loss Prev Process Ind 2023;84:105124.

[30] Yang JF, Wang PC, Liu XY, et al. Analysis on causes of chemical industry accident from 2015 to 2020 in Chinese mainland: a complex network theory approach. J Loss Prev Process Ind 2023;68:104322.

[31] Adedigba SA, Khan K, Yang M. An integrated approach for dynamic economic risk assessment of process systems. Process Saf Environ Prot 2018;116:312–23.

[32] Leveson N, Dulac N, Zipkin D, et al. Engineering resilience into safety-critical systems. Boston, MA, USA: Technical Report; MIT; 2006. 2006.

[33] Hollnagel E. FRAM, the functional resonance analysis method: modelling complex sociotechnical systems. Farnham, UK: Ashgate Publishing; 2012.

[34] Fu G, Xie X, Jia Q, Li Z, Chen P, G Y. The development history of accident causation models in the past 100 years: 24 model, a more modern accident causation model. Process Saf Environ Prot 2020;134:47–82.

[35] Studic M, Majumdar A, Schuster W, et al. A systemic modelling of ground handling services using the functional resonance analysis method. Transp Res Part C Emerg Technol 2017;74:245–60.

[36] Saurin TA, Patriarca R. A taxonomy of interactions in socio-technical systems: a functional perspective. Appl Ergon 2020;82:102980.

[37] Yu MX, Erraguntla M, Quddus N, Kravaris C. A data-driven approach of quantifying function couplings and identifying paths towards emerging hazards in complex systems. Process Saf Environ Prot 2021;150:464–77.

[38] Leveson NG. Engineering a safer world, systems thinking applied to safety. The MIT Press; 2011. p. 608. ISBN-10:0e262-01662-1, ISBN-13:978-0-262-01662-9.

[39] Kim YC, Yoon WC. Quantitative representation of the functional resonance analysis method for risk assessment. Reliab Eng Syst Saf 2021;214:107745.

[40] Jing K, Du XR, Shen LX, Tang L. Robustness of complex networks: cascading failuremechanism by considering the characteristics of time delay and recovery strategy. Phys A 2019;534:122061.

[41] Wu YP, Chen ZL, Zhao XD, Gong HD, Su XC, Chen YC. Propagation model of cascading failure based on discrete dynamical system. Reliab Eng Syst Saf 2021; 209:107424.

[42] Bruneau M, Chang SE, Eguchi RT, Lee GC, O'Rourke TD, Reinhorn AM, Shinozuka M, Tierney K, Wallace WA, Von Winterfeldt D. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq Spectra 2003;19:733–52.

[43] Sharma N, Tabandeh A, Gardoni P. Resilience analysis: a mathematical formulation to model resilience of engineering systems. Sustain Resilient Infrastruct 2018;3:49–67.

[44] Sharma N, Tabandeh A, Gardoni P. Regional resilience analysis: a multiscale approach to optimize the resilience of interdependent infrastructure. Comput Aided Civ Infrastruct Eng 2020;35:1315–30.

[45] Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. Reliab Eng Syst Saf 2011;96:925–32.

[46] Smith D, Veitch B, Khan F, Taylor R. Understanding industrial safety: comparing Fault tree, Bayesian network, and FRAM approaches. J. Loss Prev. Process. Ind. 2017;45:88–101.