A STAMP-based approach to quantitative resilience assessment of chemical process systems

Sun, H.; Wang, Haiqing; Yang, Ming; Reniers, Genserik

DOI
10.1016/j.ress.2022.108397

Publication date
2022

Document Version
Final published version

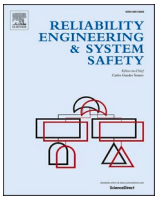
Published in
Reliability Engineering and System Safety

Reliability Engineering and System Safety 222 (2022) 108397

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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



A STAMP-based approach to quantitative resilience assessment of chemical process systems

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

[a] College of Mechanical and Electronic Engineering, China University of Petroleum (East China), Qingdao, 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] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000, Antwerp, Belgium
[d] CEDON, KULeuven, 1000 Brussels, Belgium

ARTICLE INFO

Keywords:
STAMP
Resilience assessment
Systemic
Chemical process systems

ABSTRACT

Chemical process systems (CPSs) involve complex dynamic processes. Besides, the emergent and uncertain hazards and disruptions cannot be identified entirely and prevented by conventional methods. In those situations, resilience for CPSs plays an essential role in absorbing, adapting to disruptions, and restoring from damages. Systemic modeling plays a vital role in assessing resilience. A system-based analysis model, system-theoretic accident model, and process (STAMP) can provide a robust framework. This paper develops a comprehensive methodology to systematically model and assess system resilience. The STAMP is employed to model and analyze the system safety of a process system. A new method of dynamic resilience assessment is then proposed to quantify the resilience of the system. The proposed method is applied to the diesel oil hydrogenation system. The results show that it quantifies the resilience of complex process systems considering human and organizational factors in a dynamic manner.

1. Introduction

1.1. Resilience and literature review

Given the rapid development of highly complex chemical process systems, more attention should be devoted to resilience analysis in the process industries. Subsystems and components of the process system are highly coupled and interdependent. Additional social factors (e.g., management, policy, human, and organizational factors) and their interactions with technological factors (e.g., equipment failure, process parameter variation) make the systems much more complex. Although many efforts have been made to prevent accidents, escalations, and domino effects, accidents still occur due to various social and technological factors [1–3]. Even under a rigorous risk management program, accidental disturbances not absorbed by the system may still lead to catastrophic consequences [4]. This indicates that while preventing accidents, it is also essential to handle uncertain disturbances, emergency events, and system state changes to ensure that the system operates within the set target threshold (i.e., safe state). Resilience analysis was motivated by a general unease with the inadequacy of earlier safety approaches, such as event chain models of accident causality, probabilistic risk analysis, and reliability methods [5]. Resilience assessment is more dynamic and more suitable than risk assessment to dispose of complex systems after uncertain disruptions because it is concerned not so much with the reliability of individual components but with understanding and facilitating a system's ability to actively ensure that systems do not get out of control [5–8]. Especially in dealing with emergency events and disruptions, building a resilient system is more appropriate than risk assessment. Risk management aims at preventing accidents and reducing the consequences of accidents. Resilience assessment intends to improve the ability of the system to respond to emergencies, such as prediction, absorption, adaptation, and recovery. Resilience assessment extends the conventional risk assessment to the post-accident stage. It evaluates the system's ability to anticipate, absorb, adapt to disruptions and recover from failures and accidents Zio [9].

As a new research paradigm within the field of safety science, peer researchers proposed different resilience quantification methods based

* Corresponding author at: College of Mechanical and Electronic Engineering, China University of Petroleum (East China), Qingdao, China.
** Corresponding author at: Faculty of Technology, Policy, and Management, Delft University of Technology, The Netherlands.
E-mail addresses: wanghaiqing@upc.edu.cn (H. Wang), m.yang-1@tudelft.nl (M. Yang).

https://doi.org/10.1016/j.ress.2022.108397
Received 23 May 2021; Received in revised form 12 January 2022; Accepted 13 February 2022
Available online 15 February 2022

on the characteristics of various fields [2,10–17]. Hollnagel (2011) defined the concept of resilience engineering for the first time, in which resilience was defined as "the ability that makes a system both safe and efficient, allowing it to maintain and recover a dynamic state of equilibrium while keeping functioning after a mishap or under permanent stress". By accepting the nature of resilience, the focus turns to effectively discovering interdependent factors and interactions in the system, thereby creating a more flexible and resilient process. Hosseini and Barker [14] proposed a new method to quantify resilience as a function of absorptive, adaptive, and restorative capacities using Bayesian networks. The example of an inland waterway port is used to demonstrate the method. Leveson et al. [18] employed the STAMP model to assess system resilience through utilizing it to the safety culture of the NASA Space Shuttle program. Beach et al [19]. used STAMP to qualitatively analyze the resilience of a complex cyber-physical system. Poulin and Kane [20] developed a taxonomy for infrastructure resilience by comparing 274 articles. Yang et al [21]. proposed a comprehensive approach based on deterministic and probabilistic metrics to assess the resilience of the equipment system. To prevent escalation of accidents of chemical process system, Sun et al [3]. developed a comprehensive approach based on resilience engineering and dynamic Bayesian network to assess the performance of safety barriers for chemical process system. The results show that the proposed method can be used to quantify each safety barrier's performance and enhance the safety management strategy to prevent and mitigate the escalation of accidents. Cincotta et al. [22] proposed a methodology to increase the resiliency of process plants by considering both the vulnerability and recoverability phases to prevent fire domino effects. Kammouh et al [23]. developed a novel method to evaluate the time-dependent resilience of engineering systems using resilience indicators. Mottahedi et al [24]. presented a novel methodology, considering unavailable data, to quantify the resilience of infrastructure systems by using expert judgment and fuzzy set theory. Cai et al [25]. proposed a new availability-based engineering resilience metric and considered resilience as an intrinsic ability and an inherent attribute of an engineering system. Zhang et al [26]. introduced a hybrid method based on a finite element model and dynamic Bayesian network to design a general resilience assessment approach for mechanical structure. More relevant research in chemical process systems (CPSs) can be seen in Table 1. Although the works described above show significant progress on resilience assessment, most previous studies believed that resilience is the static property of a system, which fails to reflect the highly interdependent and complex property of technical, organizational, and human-made factors in the chemical process industry.

1.2. IRML method and corresponding limitations for resilience assessment

Infrastructure Resilience-Oriented Modelling Language (IRML) is a graphical method to model and assess system resilience. It is capable of representing the system structure and functional dependencies. IRML is a comprehensive method comprising four main parts: system representation, structure analysis, qualitative analysis, and quantitative resilience assessment [35]. More details about IRML can be seen in Filippini and Silva [36]. Although it is a hybrid method for resilience assessment, some limitations limit its application. Firstly, in terms of system modeling, it can simplify the complex and nonlinear system to provide a better understanding. As a price, however, it sacrifices the accuracy and the level of detail of the representation [36]. Besides, it cannot consider the feedback and complex relationships among components. In other words, IRML is not a systems-theoretic method, which makes it different to accurately reflect the dependencies and interactions among subsystems and components in complex systems. Secondly, it quantifies the resilience of the system by adding up the functionality or performance status of each subsystem. According to the relevant literature on resilience engineering, however, resilience is expressed by the ratio of the area at the bottom of the performance curve to the total area rather than

Table 1
A summary of resilience studies for chemical process systems.

References	Research fields	Methods	Advantages
Gong and You [27,28]	Resilience optimization of CPSs	Multiobjective two-stage adaptive robust mixed-integer fractional programming (ARMIFP) model.	This method can combine the resilience assessment with corresponding resilience improvement strategies to ensure maximum resilience and minimum total capital cost under the worst-case scenario.
Azadeh et al [29].	Performance evaluation of safety and human resources of CPSs	Questionnaires and data envelopment analysis (DEA).	Discussing the performance of the resilience assessment and the integrated resilience assessment.
Jain et al [30].	Process upset events prediction analysis of CPSs	Process Resilience Analysis Framework (PRAF); Bayesian deep learning.	It improves PRAF and integrates technical factors with social factors; it can predict uncertain disruptions.
Jain et al [31].	Maintenance strategy optimization of CPSs	Process Resilience Analysis Framework (PRAF); Bayesian regression.	The proposed method improves PRAF and integrated technical factors with social factors; It can be used to determine the optimal maintenance policy for optimal and safer plant operations.
Jain et al [32].	Uncertain disruptive events prediction of the chemical and pharmaceutical industry	Process Resilience Analysis Framework (PRAF); Monte Carlo Markov Chain (MCMC); Global sensitivity analysis (GSA)	The proposed approach employed information of their process plant to make decisions rather than historical databases; It can solve two types of uncertainty: i) process-inherent uncertainty, and ii) external or unknown disruptions.
Zinetullina et al [33]. Chen et al [34].	Quantitative Resilience assessment of CPSs	Functional Resonance Analysis Method (FRAM); Dynamic Bayesian network (DBN).	The proposed approach used FRAM to determine the root causes of the accident, enhancing the accuracy of the DBN model.

(continued on next page)

Table 1 (*continued*)

References	Research fields	Methods	Advantages
	Hazardous material (HAZMAT) storage resilience assessment of chemical plants	TNT equivalency method; Heat radiation model; Stochastic dynamic algorithm.	They proposed dividing resilience metric into four parts (i.e., resistance, mitigation, adaptation, and restoration) and quantifying their capacity; It can be used to enhance storage policy and prevent domino effects.

a simple addition of performance [34].

To overcome those two shortcomings, we proposed a resilience assessment approach using the STAMP model and a new resilience metric Section 2.1 discusses how it works. A new quantification method for system resilience is developed to measure system resilience Section 2.2.2 presents this method.

1.3. STAMP model for resilience assessment

STAMP was introduced by Leveson [37] to investigate the highly complex socio-technological interactions qualitatively. According to STAMP, system safety can be viewed as a control problem. The cause of the accident is unexpected interactions between subsystems and components that violate safety constraints. STAMP has been proven to be an effective method to analyze safety in a highly complex system, and widely applied in various fields, such as water contamination accidents, railway accidents, aviation, financial crises, medical industry, and long-distance pipeline transportation industry [38–44]. Performing STAMP analysis in the initial stage of the quantitative resilience assessment of the complex systems can more strictly analyze the non-linear interdependent factors and interactions between complex technical-human-organizational factors to better reflect the situation in the system. STAMP can be employed to model the system systematically. However, it is a qualitative approach.

1.4. Objective and organization of the study

Inspired by the quantitative method of IRML, this study aims to propose a comprehensive approach, including the STAMP model and a novel resilience metric, to assess the dynamic resilience of complex systems, in which the complex interactions and interdependency among subsystems and components are considered. Besides, the influence of information feedback on the system resilience is included in the proposed methodology. We adopted a two-step method: First, STAMP is used to systematically analyze a process system's safety. Second, the dynamic resilience assessment method is proposed to quantify the resilience of the STAMP model.

The remaining parts of this paper are organized as follows. The proposed methodology of dynamic resilience assessment is presented in Section 2. The application of this approach to the diesel oil hydrogenation system is presented in Section 3. Section 4 compares the proposed method with the IRML method for assessing system resilience behavior. Finally, conclusions are drawn in Section 5.

2. The proposed methodology

The methodology is developed in this section to assess the system resilience under the influence of disruption, which includes two main parts: modeling the system using STAMP and developing a novel resilience metric to quantify the system's resilience.

Firstly, the safety constraints, control loops, process model, and control structure should be identified to model the system. In this step, the system-theoretic process analysis (STPA) is used to identify system hazards and accidents, construct control structures, determine potential unsafe control actions, and find out the causes of dangerous control actions (UCA). After that, a STAMP model is built. Then, the modeling parameters and the formula of system resilience should be determined to quantify the system resilience. Each step of the methodology is discussed in detail in the following section. The specific process is shown in Fig. 1.

2.1. STAMP modeling

In system and control theory, STAMP views the highly complex system as a combination of dependent subsystems and components, maintaining a dynamic equilibrium state through information and control feedback loops. STAMP defines safety management as a continuous control task rather than preventing component failure events from imposing necessary constraints to limit safety changes and adaptations of system behavior [37]. STAMP consists of three main concepts: safety constraints, control loops, and process models, and control structure.

(1) Safety constraints are measures that must be imposed on a system to ensure the system operates within a safe range. Accidents may occur if there are no safety constraints or the safety constraints fail to control the hazards.

(2) Control loops can conceptualize the system as a control system. The safety constraints, logic control, and information feedback in the control loops are critical to ensure system safety. The basic control loop of STAMP can be seen in Fig. 2. It consists of five main elements: controller, process model, actuator, controlled process, and sensor.

(3) In system theory, the system is regarded as a hierarchical structure. In this structure, each level imposes constraints on the activities of the levels below it. That is, constraints at higher levels or lack of

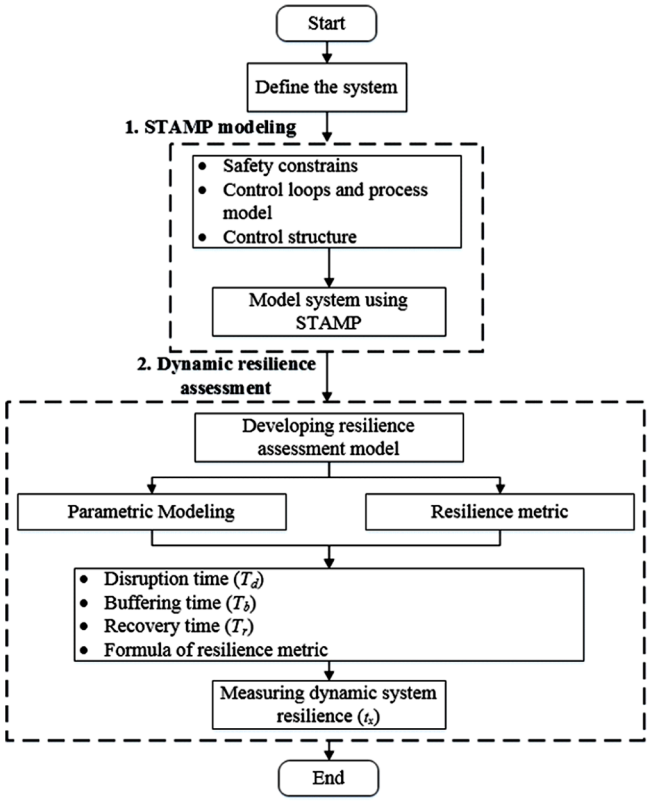


Fig. 1. The proposed methodology for assessing the system resilience.

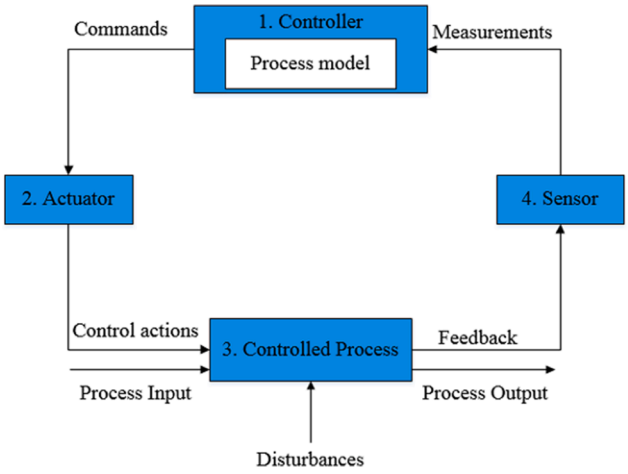


Fig. 2. The basic control loop of STAMP [45].

constraints allow or control lower-level behavior [37,46]. In the light of the control structure, the roles and responsibilities of each element of STAMP can be determined.

2.2. Dynamic resilience assessment

STAMP is an effective method to model a process system. IRML can simulate the system's response to failure propagation to check whether the system can handle the disruptions [36]. Besides, IRML facilitates the identification of functional relationships among components. However, this method transforms the system model into a more straightforward and neutral dependency network [36] to omit details of the system and subsystems. Besides, it cannot consider the complex interactions and feedback information of components and subsystems. Therefore, we use STAMP to model the system systematically. Based on this, a comprehensive method, including a novel resilience metric, is proposed to assess the dynamic resilience of process systems, which is shown in Section 2.2.2.

The proposed method simulates the response of a system to a disturbance, which may affect one or multiple nodes. This method was developed based on nodes simulation through the STAMP model. Every node is associated with a dynamic behavior in response to disturbance (buffering) or recovery from failure. The quantitative method consists of two main parts: i) determination of disruption duration (T_d), buffering time (T_b), and recovery time (T_r), and ii) resilience assessment.

2.2.1. Resilience metric of IRML

In the first part, the main task is to assign numerical values to time parameters (T_d, T_b, and T_r). The disruption duration (T_d) refers to the time period from the moment the disruption is imposed on the initial node to the moment that the disruption withdraws. The buffering time (T_b) is the interval from the time when disruption affects the node to the time when this node fails. It represents the ability of a node to resist disruptions. T_b can be regarded as the capacity of a node to absorb and adapt to disruptions. Recovery time (T_r) represents the time interval between the start of maintenance and the restoration of a node to the node's recovery. It indicates the recovery ability of node, determined by maintenance resources (e.g., maintenance policy, maintenance personnel, respond speed, etc.) of the system. It is worth noting that those parameters can be obtained from the operational data of the plant. There are four assumptions to note in this part:

- Assumption 1: As long as the disruption persists, only failure events are active in the model. Only when the disturbance stops, nodes will start to recover [36]. This is because if a node is repaired before the disruption disappears, the existing disruption will continue to affect the node.
- Assumption 2: The node can be restored only when its parent nodes are restored to the original state.
- Assumption 3: If the time for the last node in the system to recover to its original state is greater than the time for the first node affected by disruption to fail for the second time, the system cannot be restored to its original state and will fall into a loop. This indicates that the existing maintenance resources are insufficient to deal with the impact caused by the disruption on the system, and additional maintenance resources (such as professional rescue teams, government support, etc.) are needed to help the system restored to its original state.
- Assumption 4: If the system falls into a loop, to avoid overestimating the resilience, we only quantify the system resilience of the time interval from t_0 to t_x. The t_x indicates the moment when the system is restored to its original state. For a system trapped in a loop, the t_x refers to the moment when the initial node fails for the second time.

In the second part, the simple metric of system resilience can be represented as the sum of the subsystems' functionality state [36], as shown in Eq. (1):

$$r(S) = s\_1 + s\_2 + \cdots + s\_n \tag{1}$$

where S represents the system, $r(S)$ indicates the resilience of the system, n represents the number of the subsystem, s_n represents the functionality state of the subsystem n. The functionality state of subsystem can be binary, i.e., 0 and 1. 0 represents the failure of a subsystem, and 1 indicates the subsystem is functioning. Filippini and Silva [36] described the specific process of the quantitative method of IRML in their paper.

2.2.2. The proposed resilience metric

With various combinations of the functionality states of sub-systems, it only represents the system functionality. In this paper, resilience is seen as a system's ability to actively ensure that the system does not operate out of control. Therefore, a novel resilience metric should be proposed to quantify resilience for complex systems. In the light of the resilience framework proposed by Bruneau et al [47]., resilience can be expressed as Eq. (2).

$$R\left(t|e^l\right) = \frac{\varphi(t|e^l) - \varphi(t_d|e^l)}{\varphi(t_0) - \varphi(t_d|e^l)} \tag{2}$$

where $R(t|e^l)$represents the resilience at time t; e^l refers to the disruption event l;$\varphi(t|e^l)$is the functionality of the system at time t; $\varphi(t_d|e^l)$ indicates the system's lowest functionality (0 in this paper); $\varphi(t_0)$ is the system's initial functionality before the occurrence of disruption Eq. (2). can be converted into Eq. (3) by integrating Eq. (2) on the time term.

$$R(S) = \frac{\int_{t_0}^{t_x} R(t)dt}{R(t_0)(t_x - t_0)} \tag{3}$$

where$R(S)$is the system resilience; $R(t)$represents the functionality function of the system; $R(t_0)$ is the system's initial functionality before the occurrence of disruption (1 in this paper); t_x is the time that the system functionality is fully recovered; t_0 is the time that the disruption occurs.

The IRML method only considers the subsystems in the system, and the interaction of components in the subsystems is omitted. Besides, it uses the sum of functionality to express resilience directly. Those will lead to an inaccurate resilience assessment. To overcome the deficiencies of IRML, we take into account Eq. (3) and the components states of subsystems; therefore, Eq. (1) can be replaced by Eq. (4).

$$R(t) = \left[\frac{\sum_{j=1}^{m1} s_{1m1}(t)}{m1} + \frac{\sum_{j=1}^{m2} s_{2m2}(t)}{m2} + \cdots + \frac{\sum_{j=1}^{mi} s_{nmi}(t)}{mi}\right] \Big/ i \tag{4}$$

where i represents the system consists of i subsystems, the subsystem n consists of mi components, and the subsystem state can be represented as the average of the components' state. Therefore, the system resilience can be represented as Eq. (5).

$$R(S)=\frac{\int_{t_0}^{t_x}\left[\frac{\sum_{j=1}^{m1}s_{1m1}(t)}{m1}+\frac{\sum_{j=1}^{m2}s_{2m2}(t)}{m2}+\cdots+\frac{\sum_{j=1}^{mi}s_{nmi}(t)}{mi}\right]\Big/ idt}{R(t_0)(t_x-t_0)} \tag{5}$$

To illustrate this method, a simple example is given here to explain its calculation process. We take the simple STAMP model in Fig. 2 as an example to demonstrate the application of the method. There are four nodes in Fig. 2, and the time parameters are assigned to these four nodes, respectively, which is the first part of this quantitative method. Note that the time parameters are determined by practitioners based on the real situations (e.g., maintenance resources) when using the proposed method. For a simple presentation of the proposed method, assuming that the disturbance occurs at node 3; A step function is considered, which goes from 0 to 1 at time T_0=1 [36]; The T_d, T_b, and T_r are 2, 1, 1 (time unit is set in terms of an hour). The response of the nodes in the system is shown in Table 2. According to Table 2, the functionality variation is shown in Fig. 3. In the light of Eq. (5) and Fig. 3, the resilience behavior of the example model can be seen in Fig. 4.

It can be seen from Fig. 3 and Fig. 4: it took 5 h from the change in system resilience to enter a loop. When the disturbance occurs at node 3 at T_0 (1 hour), the system functionality is not immediately affected. This is because of the buffering time (T_b) of node 3, during which the influence of the disturbance is absorbed partially, and the system adapts to the disrupted condition to some extent. If no external interventions (e.g., maintenance) are taken during this time period, node 3 will fail after the T_b ends. When node 3 fails, the failure will propagate to node 4 through the shortest path, (there is only one path, i.e., 3→4). While T_b of node 4 can also absorb and adapt to the disturbance for a certain period (1 hour), then node 4 fails. The failure will then propagate to node 1 at the fourth hour. Meanwhile, node 3 recovers at the fourth hour, since $T_0+T_d+T_{r3}$=4. Simultaneously, when node 3 fails and node 4 recovers, the effects of the two nodes on the system functionality are counteracted. The term of 'jump' is introduced to represent this phenomenon. This phenomenon also occurs at the fifth hour, because at this moment node 2 fails and node 4 recovers. The rest can be done in the same manner.

It is worth noting that Fig. 2 is a directed and cyclic network due to the feedback. If node 2 recovers, its failure is propagated to node 3, the recovery process of the system will continue to circulate. In other words, the time when node 3 fails for the second time is: $T_{f32}=T_0+T_{b3}+T_{b4}+T_{b1}+T_{b2}+T_{b3}$, while the recovery time of node 2 is: $T_{2r}=T_0+T_d+T_{r3}+T_{r4}+T_{r1}+T_{r2}$. If T_{f32} is bigger than T_{2r}, the system can recover to its original state. If T_{f32} is less than T_{2r}, the failure propagation will start again, called 'Loop' in this paper. We define the recovery time of the last node of the system (node 2 in this case) as t_x. To avoid overestimating the resilience, we only quantify the system resilience of the time interval from t_0 to t_x, which is assumed in A4 in Section 2.2.1.

According to the definition mentioned above, it can be seen from Table 2 that the $T_{f31}=T_0+T_{b3}$=2, which means that the first failure time of node 3 is 2 h. While, the second failure time of node 3 is: $T_{f32}=T_{f31}+T_{b4}+T_{b1}+T_{b2}+T_{b3}$=6. $T_{2r}=T_0+T_d+T_{r3}+T_{r4}+T_{r1}+T_{r2}$=7, this means that this system cannot restore to its original state within those kinds of time parameters (i.e., T_0=1, for T_d, T_b, and T_r are 2, 1, 1), which is shown in Fig. 4. In other words, as described in A2 and A3 in Section 2.2.1, before node 2 recovers to its initial state, the effects of its failure propagated to node 3, causing node 3 to fail for the second time. Therefore, the system resilience will fall into a loop. The end state of the system functionality is 0.75, while the end state of the system resilience is 0.871. It is worth noting that some repaired nodes may fail again before the entire system is repaired. Thus, the system cannot be restored to its previous state. Unless the buffering time of the node is increased or the repair time of the node is reduced (e.g., S21 and S31 in Fig. 8 and Fig. 9), achieving these requires additional maintenance resources, like government support.

3. Case study

3.1. Description of diesel oil hydrogenation system

The process of diesel oil hydrogenation illustrates the proposed methodology, as shown in Fig. 5. Diesel oil first enters the buffer tank to avoid pump cavitation. Then it is mixed with hydrogen in a mixer. The mixed gaseous hydrogen and liquid diesel fuel are preheated through heat exchangers and enter the furnace. The mixture is heated to a certain temperature and then enters the reactor. The product of the reactor is cooled to 49 °C and then enters the high-pressure separator. High-purity hydrogen is generated at the top of the separator. Most of the gas is returned to the furnace as recycled hydrogen. The hydrogenated oil is separated from the middle of the high-pressure separator and enters the low-pressure separator. Due to the decrease in pressure, the hydrogen and low-molecular hydrocarbons dissolved in the oil are separated from the oil. The refined oil finally enters the fractionating tower. Various hydrocarbons will be produced at the top of the tower, and multiple products will be produced at the bottom of the tower. The specific process is shown in Fig. 5.

It is worth noting that pressure control is essential during the whole process. Because the pressure in the buffer tank is about 0.38 MPa, while the pressure in the furnace and reactor is very high, up to 5.7 MPa. If the pressure in the reactor flows back into the buffer tank, it will cause excessive pressure in the buffer tank, and an explosion will happen. For example, on March 12, 2018, a buffer tank exploded in the diesel oil hydrogenation process system and caused a massive fire at the Jiujiang petrochemical company in Jiujiang, Jiangxi, China [48,49]. The main cause of the accident was the pressure flow-back, which caused the pressure in the buffer tank to surge beyond its design pressure. In this paper, the pressure control system of the diesel oil hydrogenation process system is utilized to illustrate the proposed methodology.

3.2. The stamp modeling

Before assessing the resilience of the pressure control system for the

Table 2
The response of each node.

Node	Parameters	Pre-disruption	The moment when the disruption affects the nodes (hour)	Fail	Recover
1	Timepoint	–	$T_0+T_{b3}+T_{b4}$	$T_0+T_{b3}+T_{b4}+T_{b1}$	$T_0+T_d+T_{r3}+T_{r4}+T_{r1}$
	Node state	1	1	0	1
2	Timepoint	–	$T_0+T_{b3}+T_{b4}+T_{b1}$	$T_0+T_{b3}+T_{b4}+T_{b1}+T_{b2}$	$T_0+T_d+T_{r3}+T_{r4}+T_{r1}+T_{r2}$
	Node state	1	1	0	1
3	Timepoint	–	T_0	T_0+T_{b3}	$T_0+T_d+T_{r3}$
	Node state	1	1	0	1
4	Timepoint	–	T_0+T_{b3}	$T_0+T_{b3}+T_{b4}$	$T_0+T_d+T_{r3}+T_{r4}$
	Node state	1	1	0	1

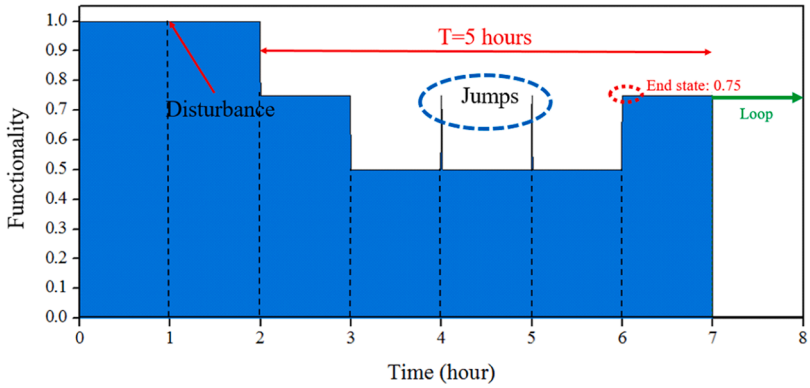


Fig. 3. The functionality behavior of the example model.

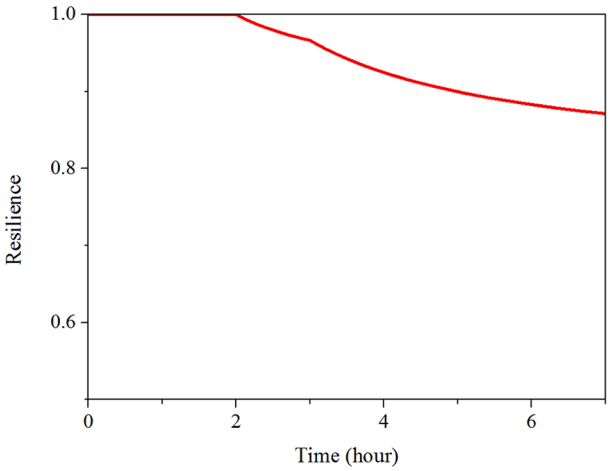


Fig. 4. The system resilience behavior of the example model.

diesel oil hydrogenation system, it is necessary to model the system. STAMP is used to model the system, and STPA is used to identify system hazards.

In this case, the system has the characteristics of high temperature, high pressure, flammability, and explosiveness. Two unexpected events are critical. The first is a physical explosion caused by high pressure, such as the aforementioned Jiujiang accident. The second one is leakage, which may lead to accidents, like fire, explosion, or contamination. Therefore, the high-level hazards of the system related to those two unexpected events are high pressure, flow rate, and liquid level in the system and devices. Keeping those variables within the safe range is the safety constraint of the system. For illustrative purpose, analysis is conducted based on the pressure control system of the diesel oil hydrogenation process system in this paper, which means that pressure is the critical variable.

Before identifying the system control structure, the first task to be conducted is to determine the entities and their roles in the system. For this study, the facility includes a buffer tank, valves, pump, furnace, reactor, recycle hydrogen compressor, and controllers. The controllers include indicators, alarms, and controllers for main variables (e.g., temperature, pressure, level). The main task of controllers is to keep the variables in the process of diesel hydrogenation within the set value or certain range to ensure system safety. The specific facilities and their roles are shown in Table 3. According to the STAMP and STPA method, the system control structure of the pressure control system is shown in Fig. 6.

To ensure system safety, the operation and process parameters must be monitored and controlled. Besides, unsafe control actions (UCA) should be identified. According to the pressure control system of the diesel oil hydrogenation process system, all components (e.g., corporate, plant manager, controller, actuator, and sensor) and their interactions should be considered. The UCAs can be divided into four categories; namely, control action required for safety is not provided, control action is unsafe, control action required for safety occurs too early or too late, and control action required for safety is stopped too soon or applied too long, respectively [37]. The specific UCAs and their causes are shown in

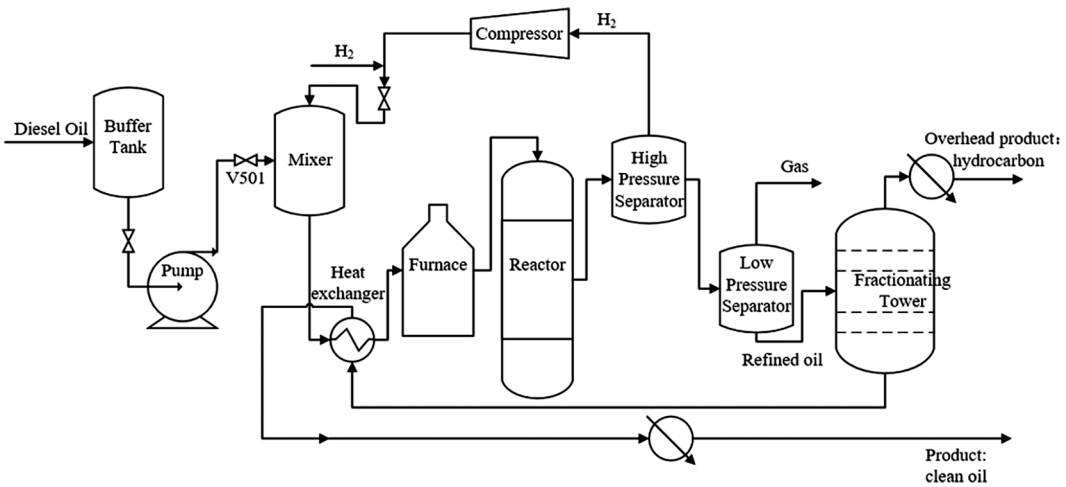


Fig. 5. Schematic diagram of the diesel oil hydrogenation process system.

Table 3
The facilities' roles of the diesel oil hydrogenation process.

Facility	Roles
Buffer tank	Protects pumps Relief valve: open the valve to reduce the pressure or temperature in the container when the variable exceeds the threshold; Emergency shut down valve: when the system is abnormal, the valve is used to cut off the process to isolate the unit; Safety valve: open the valve to reduce the pressure or temperature in the container when the variable exceeds the threshold
Valves	
Pump	Pumps diesel oil from the buffer tank into the mixer
Mixer	Mixes diesel oil and gaseous hydrogen
Heat exchanger	Preheats the mixture
Furnace	The mixture of diesel and hydrogen is heated to a specific temperature
Reactor	Hydrogenation reaction in the presence of the catalyst
Compressor	Maintains a high pressure in the reaction system; recycle hydrogen from the separator
Indicators	Displays variables in the system or device (local and at control room)
Alarms	Requires emergency action by an operator (site operator or control room operator) to reduce or shutdown inflow
Controllers	Reduces or stops inflow by the automatic controller (DCS or SIS)

Table 4.

3.3. Dynamic resilience assessment using STAMP

The STAMP model of the pressure control system for the diesel oil hydrogenation system is constructed in the previous section. In the light of the principle technological procedure described in Section 2.2, the task of this part is to conduct the dynamic resilience assessment for STAMP. Assume that the disruption occurred at the controller in the control room (i.e., node 3). Engineers can determine the location of disruption based on real situations and requirements when using this method. It is worth noting that since node 3 issued the wrong command, and the command was transmitted to the node below node 3, node 1 and 2 are functioning before the feedback information from node 11 reaches node 3. When the disruption occurs at node 3, the remaining nodes in the system may be affected, that is, system response. Node 4, node 5, node 6, node 7, node 8, node 9, node 10, and node 11 are the potentially affected nodes.

As can be seen from Fig. 6, each node is affected by different nodes. Since each node has a different buffering time (T_b) and recovery time (T_r), nodes are affected to different degrees. Those parameters can be obtained from the actual data and operational records of the plant. For example, maintenance data are recorded in the plant, so T_b is the time interval from initial installation to failure time, and T_r is the time interval from the start of maintenance to the recovery to normal state. T_0 represents that a disruption event occurs at node 3 after the system runs for $T_{0\ \mathrm{min}}$ (10 min in this paper). Due to the lack of actual data on the process parameters of the pressure control system, to illustrate the application of the proposed methodology, the assigned value of T_d, T_b and T_r are shown in Table 5.

Due to the interaction between components in the system, disruption affects nodes in multiple paths. For example, node 3 is affected by the disruption and by node 11 (i.e., information feedback), which means that the child node of a node in the STAMP model may also be the parent node of the node. In other words, the proposed method considers the interaction between components and considers the influence of information feedback on components. This is the difference between the proposed method in this paper and the IRML method.

When the node starts to be affected by the disruption, its state will change. Since a node may be affected by multiple nodes, there are many paths for disruption to propagate to a node. The disruption will propagate to the downstream nodes in the shortest path. A failed node may recover if the disturbance stops, which means that all ancestor nodes have recovered in their turn [36]. If the recovery speed of the system is less than the fault propagation speed, the system will fall into a loop or breakdown, which is described in A4 in Section 2.2.1. For example, when node 11 fails, the fault will propagate to node 3. If the nodes in the system are not fully recovered before node 3 fails a second time, the

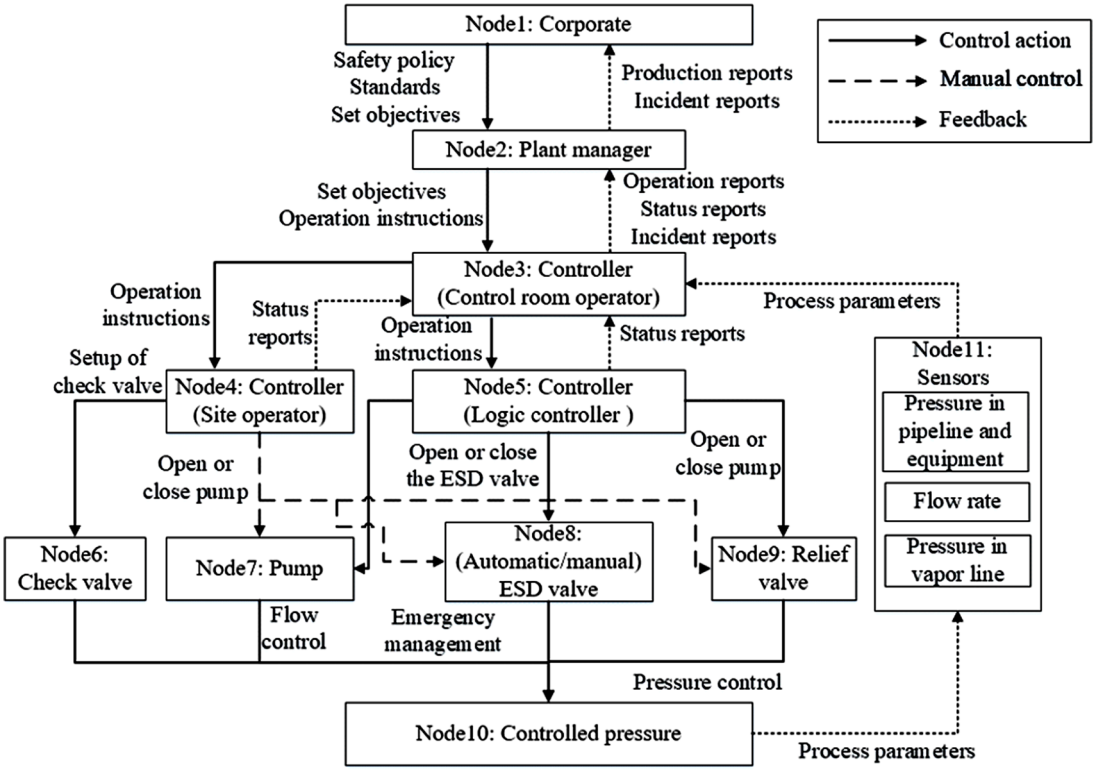


Fig. 6. The control structure of the pressure control system of the diesel oil hydrogenation process system.

Table 4
The UCAs for the pressure control system.

Category	UCAs	Causal factors	Safety constraints
Control action is not provided	The emergency shutdown valve at the outlet of the feed pump is not provided	The design is non-standard	Management and investigation
	Sign of the high pressure in equipment and/or pipeline is not detected	Pressure indicator and alarm fail	Inspection and maintenance
	Failure of the check valve is not detected	Operators lack of skill and experience	Safety training
	Failure of the relief valve is not detected	Operators lack of skill and experience	Safety training
Control action is unsafe	Failure of the check valve	The operators do not notice or check the function of the check valve	Inspection and maintenance
	The detected pressure in equipment and/or pipeline is wrong	Pressure indicators fail or operators misread pressure	Inspection and maintenance, training
Control action occurs too early or too late	Operators do not close the ESD valve in time	Operators lack of skill and experience	Safety training
	The relief valve is not opened in time	Relief valve fails	Inspection and maintenance
	The command from the control room is late	Operators at the control room lack of skill and experience	Safety training
	The abnormal pressure is not disposed in time after it is detected	The operators are negligent or lack of skill, or the emergency plan is inadequate.	Management, training, emergency exercise
Control action is stopped too soon or applied too long	–	–	–

Table 5
The assumed value of T_d, T_b and T_r.

Scenario	Variables (minute)	Constant (minute)	Description
Scenario 1	S11: T_d=10; S12: T_d=20; S13: T_d=30; S14:T_d=40	T_b=10, T_r=10	The influence of different T_d on the system resilience behavior
Scenario 2	S21:T_b=5; S22: T_b=10; S23: T_b=15; S24: T_b=20	T_d=20, T_r=10	The influence of different T_b on the system resilience behavior
Scenario 3	S31:T_r=5; S32: T_r=10; S33: T_r=15; S34: T_r=20	T_d=20, T_b=10	The influence of different T_r on the system resilience behavior

resilience behavior of the system enters a loop or completely breaks down. The specific situation depends on the buffering time (T_b) and recovery time (T_r) of each component of the system. In other words, the system will only recover completely when the total recovery time of the system is less than or equal to the total failure propagation time. The specific paths are shown in Table 6.

According to Table 5, Table 6, and the technological procedure described in Section 2.2, the state of each node in the system is shown in Table 7. The system resilience behaviors of Scenario 1, Scenario 2, and Scenario 3 are calculated based on Table 7, and the results are shown in Fig. 7, Fig. 8, and Fig. 9, respectively.

The simplified representation of the pressure control system is employed to demonstrate the proposed approach. In this study, one node (i.e., node 5 in Fig. 6) is utilized to represent the all-related logical controllers. This is a simplified representation of the control system. In reality, different and independent controller logics are used to actuate the ESD and safety valves. It can be seen from Fig. 7, the larger the T_d (disruption duration), the smaller the resilience of the system. When T_d increases, the possibility of the system returning to its original state is

Table 6
The path of each node affected by disruption.

Node	Disruption propagation path	Nodes recovery path
1	Min(3–4–6/7/8/9–10–11–3–2–1; 3–5–7/8/9–10–11–3–2–1)	3–2–1
2	Min(3–4–6/7/8/9–10–11–3–2; 3–5–7/8/9–10–11–3–2)	3–2
3	3	3
4	3–4	3–4
5	3–5	3–5
6	3–4–6	3–4–6
7	Min(3–4–7; 3–5–7)	Max(3–4–7; 3–5–7)
8	Min(3–4–8; 3–5–8)	Max(3–4–8; 3–5–8)
9	Min(3–4–9; 3–5–9)	Max(3–4–9; 3–5–9)
10	Min(3–4–6/7/8/9–10; 3–5–7/8/9–10)	Max(3–4–6/7/8/9–10; 3–5–7/8/9–10)
11	Min(3–4–6/7/8/9–10–11; 3–5–7/8/9–10–11)	Max(3–4–6/7/8/9–10–11; 3–5–7/8/9–10–11)

Table 7
The time point and state of nodes of the system.

Node	Parameters	Pre-disruption	Fail	Recover
1	Timepoint	–	T_0+T_{b3}+Min (T_{b4}+T_{b6}/ T_{b7}/ T_{b8}/ T_{b9}+T_{b10}+T_{b11}, T_{b5}+T_{b7}/ T_{b8}/T_{b9} +T_{b10}+T_{b11})+ T_{b3}+T_{b2}+T_{b1}	T_0+T_d+T_{r3}+T_{r2}+T_r1
	State	1	0	1
2	Timepoint	–	T_0+T_{b3}+Min (T_{b4}+T_{b6}/ T_{b7}/ T_{b8}/ T_{b9}+T_{b10}+T_{b11}, T_{b5}+T_{b7}/ T_{b8}/T_{b9} +T_{b10}+T_{b11})+ T_{b3}+T_{b2}	T_0+T_d+T_{r3}+T_{r2}
	State	1	0	1
3	Timepoint	–	T_0+T_{b3}	T_0+T_d+T_{r3}
	State	1	0	1
4	Timepoint	–	T_0+T_{b3}+T_{b4}	T_0+T_d+T_{r3}+T_{r4}
	State	1	0	1
5	Timepoint	–	T_0+T_{b3}+T_{b5}	T_0+T_d+T_{r3}+T_{r5}
	State	1	0	1
6	Timepoint	–	T_0+T_{b3}+T_{b4}+T_{b6}	T_0+T_d+T_{r3}+ T_{r4}+T_{r6}
	State	1	0	1
7	Timepoint	–	T_0+ T_{b3}+ T_{b4}/T_{b5}+ T_{b7}	T_0+T_d+T_{r3}+ Max (T_{r4}+T_{r7}, T_{r5}+ T_{r7})
	State	1	0	1
8	Timepoint	–	T_0+ T_{b3}+ T_{b4}/T_{b5}+ T_{b8}	T_0+T_d+T_{r3}+ Max (T_{r4}+T_{r8}, T_{r5}+ T_{r8})
	State	1	0	1
9	Timepoint	–	T_0+T_{b3}+ T_{b4}/ T_{b5}+T_{b9}	T_0+T_d+T_{r3}+ Max (T_{r4}+T_{r9}, T_{r5}+ T_{r9})
	State	1	0	1
10	Timepoint	–	T_0+T_{b3}+Min (T_{b4}+T_{b6}/ T_{b7}/ T_{b8}/ T_{b9}, T_{b5}+T_{b7}/ T_{b8}/ T_{b9})+ +T_{b10}	T_0+T_d+T_{r3}+ Max (T_{r4}+T_{r6}/ T_{r7}/ T_{r8}/T_{r9}, T_{r5}+T_{r7}/ T_{r8}/T_{r9}) +T_{r10}
	State	1	0	1
11	Timepoint	–	T_0+T_{b3}+Min (T_{b4}+T_{b6}/ T_{b7}/ T_{b8}/ T_{b9}+T_{b10}, T_{b5}+T_{b7}/ T_{b8}/T_{b9} +T_{b10}) +T_{b11}	T_0+T_d+T_{r3}+ Max (T_{r4}+T_{r6}/ T_{r7}/ T_{r8}/T_{r9}, T_{r5}+T_{r7}/ T_{r8}/T_{r9}) +T_{r10}+T_{r11}
	State	1	0	1

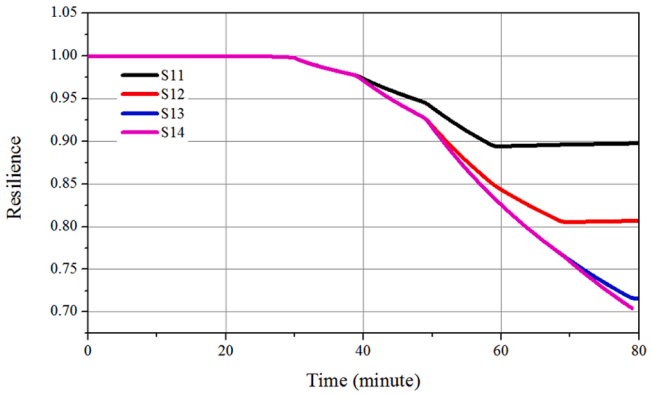


Fig. 7. The system resilience behaviors of Scenario 1.

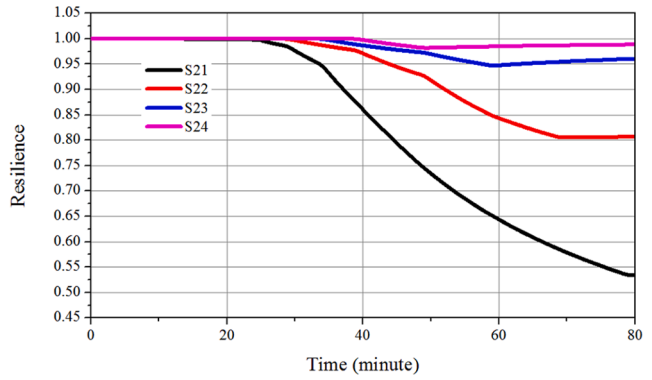


Fig. 8. The system resilience behaviors of Scenario 2.

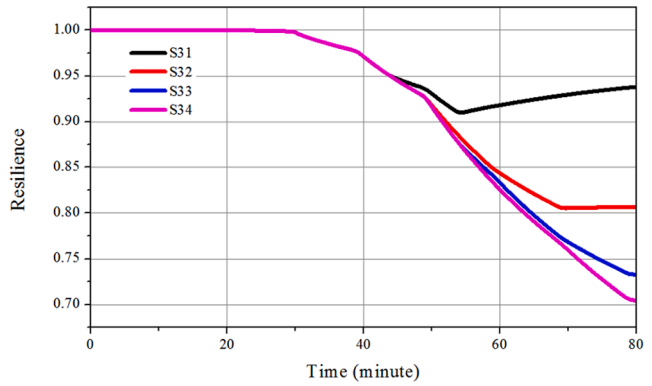


Fig. 9. The system resilience behaviors of Scenario 3.

reduced. When the buffer time and recovery time of nodes remain constant, the longer the disturbance acts on the system, the greater the influence on the system will be. Besides, the time for the system to return to a new state also increases, which means that the longer the T_d, the less safe the system. In Fig. 8, we can see that when T_b is 5, the system will fail to recover. As time goes by, the system's resilience will become 0. This is due to the short buffering time of the components. All components have failed before external measures are taken, which leads to the breakdown of the system. As a result, the longer the buffer time, the better the system resilience, and the shorter it takes for the system to return to its new equilibrium. Note that when T_b is 20 (S24 in Fig. 8), the system can be restored to its normal state, which means that the system resilience can be improved by increasing the buffering time of each component. Besides, as T_b increases from 5 to 20, the moment when the system resilience starts to rise gradually decreases, which means that the system resilience increases. For instance, when is T_b 10 min, it takes the system 70 min to start to recover. While, when T_b 15 min, it takes system 60 min to begin to recover, and this time period became 50 min when T_b increased to 20. This is because when the buffer time T_b of components becomes longer, the buffer time can be used for conducting maintenance. If the buffer time is long enough, i.e., longer than the recovery time (T_r), the fault will not propagate downstream nodes. It can be seen from Fig. 9 that the shorter the component's recovery time, the stronger the system resilience. Shortening the recovery time (T_r) of components is the second way to increase system resilience. Combining Fig. 8 and Fig. 9, it can be concluded that as long as T_b is larger than T_r, the resilience of the system is able to recover gradually. For instance, assume that a disruption occurs on a pump. If it can be repaired before the pump loses its function completely, the fault will not continue to propagate to downstream nodes. If T_b and T_r are equal, the system resilience cannot be restored to its original state 1, which can be seen in the S_{22} in Fig. 8 and S_{32} in Fig. 9.

By comparing Figs. 7-9, it can be seen that T_b and T_r have a significant impact on the system resilience behavior of the system. The smaller the recovery time of the component, the smaller the time required for the system to recover from the disturbed state to the normal state. Since the T_d cannot be controlled, the resilience of the system can be enhanced from two aspects: i) increasing the buffering time (T_b) and ii) reducing the recovery time (T_r). T_b can be increased by intrinsic safety factors, while T_r is determined by external measures. In other words, increasing T_b can fundamentally ensure system safety. Therefore, to some extent, T_b is more important than T_r. Increasing T_b can significantly enhance the resilience of the system, such as setting backup pumps, ESD valves, etc. In this way, standby equipment can be used to reduce the impact of disruptions on the system. Reducing T_r can be achieved by increasing inspection frequency and repairing in time, such as establishing relevant inspection and maintenance policies by the plant supervisor and training employees to improve their emergency response-ability (i.e., enhance the effectiveness of safety constraints in Table 4).

A resilient system may recover to a normal state as long as there is sufficient external maintenance and repairment. However, due to the system being affected by the disruption, its functionality will be reduced, which may lead to accidents. For example, in the Jiujiang accident, the accident happened when operators would close the valve. If the operator can close the valve before the explosion (i.e., if the system is more resilient or the system's functionality can be maintained at a higher level after a disruption), accidents can be avoided.

3.4. Discussion

The proposed methodology is illustrated by a simplified pressure control system. Due to the complex calculation process and for illustrative purpose, some nodes with the same function are simplified and represented by one node for the convenience of demonstrating the proposed approach. The STAMP model can be customized according to actual application conditions. To address this limitation, in future work, it is possible to design a software tool, which can automatically assign the corresponding parameter values (e.g., T_b and T_r) to all nodes in the STAMP model. In this way, the system resilience can be quantified efficiently even if the STAMP model is complex.

The main contribution of the proposed methodology is reflected in two aspects. (i) The STAMP is able to systematically analyze the interactions between components and consider the influence of information feedback on the components. However, those critical factors are ignored in IRML. To illustrate the difference, take one condition (T_d =10 min) of Scenario 1 in Table 5 as an example. In this paper, node 3 is affected by disturbance, and node 11, which considers the information feedback. However, IRML is a simplified model. It only considers the influence between the subsystems and ignores the influence of the components within the subsystem, and it cannot consider the information feedback. (ii) A novel resilience metric is proposed to quantify the

resilience of chemical process systems. IRML uses the sum of the functionality of the system to express resilience directly, which will lead to an inaccurate resilience assessment. However, system resilience represents the ability of absorption, adaptation, and restoration for the system, rather than the functionality or reliability of one or more components. Therefore, a novel resilience metric is proposed to overcome the shortcoming of IRML. Hence, the proposed methodology, including STAMP and a novel resilience assessment method, provides a potential way to quantify the resilience of complex systems.

The system resilience behaviors calculated by those two different methods are shown in Fig. 10. The IRML method does not consider the influence of information feedback. Thus, the system may recover to its original state. The results obtained from the proposed method show that the system cannot recover to its original state in this scenario. This is because some repaired nodes (node 3 in this case) fail again before the entire system is repaired. In a process system, the wrong information feedback may lead to inappropriate control action and improper decisions by the controller (e.g., logical controller and operators), reducing the system performance again. Therefore, the proposed methodology fits better to the actual process system behavior. Since the STAMP model is a closed-loop model, the system resilience quantification may fall into a continuous process. There are possible solutions: i) increasing the buffering time, and ii) reducing the repair time (e.g., S24 and S31 in Fig. 8 and Fig. 9). In a real case, the wrong information feedback from the sensors (node 11 in Fig. 6) will cause the supervisor to make wrong decisions. Although the IRML method can also reflect the resilience behavior of the system as a whole, its results are somewhat inaccurate because it omits the interaction between components and the influence of information feedback.

4. Conclusions

Dynamic resilience assessment requires a rigorous analysis of the root causes of the accident. Due to a process system's highly interactive and complex characteristics, the traditional methods cannot model the system systematically. They cannot present the interactions of technical-human-organizational factors, which will lead to inaccurate resilience assessment results. The current study proposes a comprehensive approach to modeling and quantifying the dynamic resilience of complex process systems. The proposed methodology takes advantage of STAMP to consider the information feedback and determine the key variables and root constraints of the system. After that, a novel quantitative resilience assessment method is developed to quantify the temporal changes of the resilience of a complex chemical process system. The main contributions of the proposed methodology are: i) utilizing a systemic model to describe the resilience behavior of a process system (i.e., considering the complex interaction among subsystems and components and influence of the information feedback); ii) developing a new approach to measuring the dynamic resilience of the system. The detailed results provide the required measures to enhance the system resilience. The proposed method can generate a real-time resilience profile, which helps extract valuable information from operational data to improve system resilience and provide an early warning for accidents. It can also help engineers and operators to make effective decisions to prevent accidents or reduce their consequences.

CRediT authorship contribution statement

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

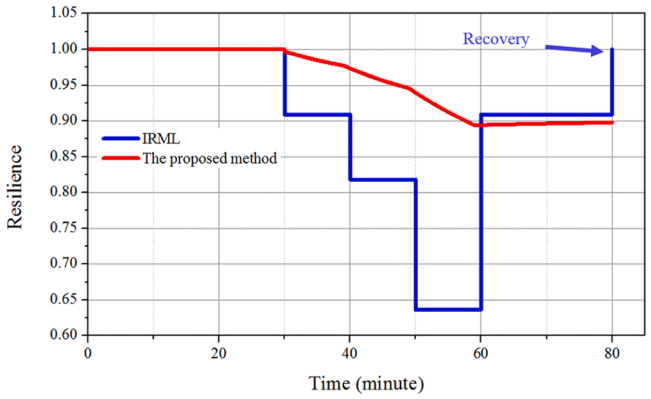


Fig. 10. The difference of system resilience behavior between the proposed method and IRML.

Declaration of competing interest

The research being report in this paper titled "**Resilience Assessment of Chemical Process Systems using System-Theoretic Accident Model and Process (STAMP)**" was supported by China University of Petroleum and Delft University of Technology. The authors of this paper have the IP ownership related to the research being reported. The terms of this arrangement have been reviewed and approved by the university in accordance with its policy on objectivity in research.

Acknowledgments

The authors gratefully acknowledge the financial support provided by the National Key R&D Program of China (No: 2019YFB2006305).

References

[1] Ding L, Khan F, Ji J. A novel vulnerability model considering synergistic effect of fire and overpressure in chemical processing facilities. Reliab Eng Syst Saf 2021. https://doi.org/10.1016/j.ress.2021.108081.
[2] Doorn N, Gardoni P, Murphy C. A multidisciplinary definition and evaluation of resilience: the role of social justice in defining resilience. Sustain Resilient Infrastruct 2019;4(3):112–23.
[3] Sun H, Wang H, Yang M, Reniers G. Resilience-based approach to safety barrier performance assessment in process systems. J Loss Prev Process Ind 2021;73:104599.
[4] Dinh L, Pasman H, Gao X, Mannan M. Resilience engineering of industrial processes: principles and contributing factors. J Loss Prev Process Ind 2012;25:233–41.
[5] Hollnagel, E., Woods, D., Leveson, N., 2006. Resilience engineering: concepts and precepts. Resilience Eng.: concept. Precept..
[6] Himoto K, Suzuki K. Computational framework for assessing the fire resilience of buildings using the multi-layer zone model. Reliab Eng Syst Saf 2021;216:108023.
[7] Liu X, Fang YP, Zio E. A hierarchical resilience enhancement framework for interdependent critical infrastructures. Reliab Eng Syst Saf 2021;215:107868.
[8] Zeng ZG, Fang YP, Zhai QQ, Du SJ. A Markov reward process-based framework for resilience analysis of multistate energy systems under the threat of extreme events. Reliab Eng Syst Saf 2021;209:107443.
[9] Zio E. The future of risk assessment. Reliab Eng Syst Saf 2018;177:176–90.
[10] Abimbola M, Khan F. Resilience modeling of engineering systems using dynamic object-oriented Bayesian network approach. Comput Ind Eng 2019;130:108–80.
[11] Cai Z, Hu J, Zhang L, Ma X. Hierarchical fault propagation and control modeling for the resilience analysis of process system. Chem Eng Res Des 2015;103:50–60.
[12] Chen CK, Xu LL, Zhao DY, Xu T, Lie P. A new model for describing the urban resilience considering adaptability, resistance and recovery. Saf Sci 2020;128:104756.
[13] Holloway T, Williams J, Ouelhadj D, Cleasby B. Process stress in municipal wastewater treatment processes: a new model for monitoring resilience. Process Saf Environ Prot 2019;132:169–81.
[14] Hosseini S, Barker K. Modeling infrastructure resilience using Bayesian networks: a case study of inland waterway ports. Comput Ind Eng 2016;93:252–66.
[15] Jain P, Rogers W, Pasman H, Mannan M. A resilience-based integrated process systems hazard analysis (RIPSHA) approach: part II management system layer. Process Saf Environ Prot 2018;118:115–24.
[16] Núñez-López J, Rubio-Castro E, Ponce-Ortega J. Involving resilience in optimizing the water-energy-food nexus at macroscopic level. Process Saf Environ Prot 2021;147:259–73.

[17] Yodo N, Wang P. Resilience modeling and quantification for engineered systems using Bayesian networks. J Mech Des 2016;138:031404.
[18] Leveson N. A systems approach to risk management through leading safety indicators. Reliab Eng Syst Saf 2015;136:17–34.
[19] Beach P, Mills R, Burferin B, et al. A STAMP-based approach to developing quantifiable measures of resilience. In: The 16th int'l conf on embedded systems, cybei-physical systems, and applocations; 2018. p. 103–9.
[20] Poulin C, Kane MB. Infrastructure resilience curves: performance measures and summary metrics. Reliab Eng Syst Saf 2021;216:107926.
[21] Yang BF, Zhang L, Zhang B, et al. Resilience metric of equipment system: theory, measurement and sensitivity analysis. Reliab Eng Syst Saf 2021;215:107889.
[22] Cincotta S, Khakzad 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.
[23] Kammouh O, Gardoni P, Cimellaro G. Probabilistic framework to evaluate the resilience of engineering systems using Bayesian and dynamic Bayesian networks. Reliab Eng Syst Saf 2020;198:106813.
[24] Mottahedi A, Sereshki F, Ataei M, et al. Resilience estimation of critical infrastructure systems: application of expert judgment. Reliab Eng Syst Saf 2021;215:107849.
[25] Cai BP, Xie M, Liu YH, Liu YL, Feng Q. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab Eng Syst Saf 2018;172:216–24.
[26] Zhang Q, Liu L, Liu Z. Application of safety and reliability analysis in wastewater reclamation system. Process Saf Environ Prot. 2021;146:338–49.
[27] Gong J, You FQ. Resilient design and operations of process systems: nonlinear adaptive robust optimization model and algorithm for resilience analysis and enhancement. Comput Chem Eng 2018;116:231–52.
[28] Gong J, You F. Resilient design and operations of chemical process systems. Comput Aided Chem Eng 2018;43:1–6. Elsevier.
[29] Azadeh A, Salehi V, Ashjari B, Saberi M. Performance evaluation of integrated resilience engineering factors by data envelopment analysis: the case of a petrochemical plant. Process Saf Environ Prot 2014;92(3):231–41.
[30] Jain P, Chakraborty A, Pistikopoulos EN, Mannan MS. Resilience-based process upset event prediction analysis for uncertainty management using Bayesian deep learning: application to a polyvinyl chloride process system. Ind Eng Chem Res 2018;57(43):14822–36.
[31] Jain P, Pistikopoulos EN, Mannan MS. Process resilience analysis based data-driven maintenance optimization: application to cooling tower operations. Comput Chem Eng 2019;121:27–45.
[32] Jain P, Diangelakis NA, Pistikopoulos EN, Mannan MS. Process resilience based upset events prediction analysis: application to a batch reactor. J Loss Prev Process Ind 2019;62:103957.
[33] 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.
[34] Chen C, Yang M, Reniers G. A dynamic stochastic methodology for quantifying HAZMAT storage resilience. Reliab Eng Syst Saf 2021;215:107909.
[35] Hu J, Faisal K, Zhang L. Dynamic resilience assessment of the Marine LNG offloading system. Reliab Eng Syst Saf 2021;208:107368.
[36] Filippini R, Silva A. A modeling framework for the resilience analysis of networked systems-of –systems based on functional dependencies. Reliab Eng Syst Saf 2014;125:82–91.
[37] Leveson N. A new accident model for engineering safer systems. Saf Sci 2004;42:237–70.
[38] Abdulkhaleq A, Wagner S, Leveson N. A comprehensive safety engineering approach for software-intensive systems based on STPA. Proc Eng 2015;128:2–11.
[39] Altabbakh H, AlKazimi MA, Murray S, et al. STAMP – holistic system safety approach or just another risk model? J Loss Prev Process Ind 2014;32:109–19.
[40] Fu G, Xie X, Jia Q, Li Z, Chen P, G Ying. 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.
[41] Ouyang M, Liu H, Yu M, Fei Q. STAMP-based analysis on the railway accident and accident spreading: taking the China-Jiaoji railway accident for example. Saf Sci 2010;48:544–55.
[42] 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.
[43] Yousefi A, Hernandez M. A novel methodology to measure safety level of a process plant using a system theory based method (STAMP). Process Saf Environ Prot 2020;136:296–309.
[44] Zhang YP, Cai BP, Liu YL, et al. Resilience assessment approach of mechanical structure combining finite element models and dynamic Bayesian networks. Reliab Eng Syst Saf 2021;216:108043.
[45] Niwa Yuji. A proposal for a new accident analysis method and its application to a catastrophic railway accident in Japan. Cognit Technol Work 2009;11(3):187–204.
[46] Checkland P. Systems thinking, systems practice. New York: John Wiley & Sons; 1981.
[47] 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. Earthquake Spectra 2003;19:733–52.
[48] Deng H. The explosion and fire accident of "3•12" petrochemical plant in Jiujiang, Jiangxi Province. Xian Dai Ban Zu. 2018;6:29.
[49] Ministry of Emergency Management of the People's Republic of China, 2019. Hazardous chemical accidents that occurred in March in history. https://www.mem.gov.cn/.