Safety Science 171 (2024) 106375

Contents lists available at ScienceDirect

Safety Science

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

Dynamic risk assessment of chemical process systems using the System-Theoretic accident model and process approach (STAMP) in combination with cascading failure propagation model (CFPM)

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

[a] School of Civil Engineering and Architecture, Anhui University of Technology, Maanshan, Anhui 243002, China
[b] College of Mechanical and Electronic Engineering, China University of Petroleum (East China), Qingdao, China
[c] Safety and Security Science Section, Department of Values, Technology, and Innovation, Faculty of Technology, Policy, and Management, Delft University of Technology, the Netherlands
[d] Centre of Hydrogen Energy, Institute of Future Energy, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia
[e] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000, Antwerp, Belgium
[f] CEDON, KULeuven, 1000 Brussels, Belgium

ARTICLE INFO

Keywords:
STAMP
Fault propagation
Cascading failure propagation model (CFPM)
Risk accumulation

ABSTRACT

To maintain continuous production, chemical plant operators may ignore faults or handle faults online rather than shutting down process systems. However, interaction and interdependence links between components in a digitalized process system are substantial. Thus, faults will be propagated to downstream nodes, potentially leading to risk accumulation and major accidents. However, limited attention has been paid to this type of risk. To model the risk accumulation process, a dynamic risk assessment method is proposed by integrating the system-theoretic accident model and process approach (STAMP) and the cascading failure propagation model (CFPM). Firstly, STAMP is used to model and analyze the system safety of a process system. Two CFPMs are then proposed to measure risk accumulation under two different engineering situations. The proposed method is applied to the Chevron Richmond refinery crude unit and its associated upstream process. The results show that the proposed approach can effectively quantify the process of risk accumulation. This method can generate a real-time dynamic risk profile to support auxiliary decision-making.

1. Introduction

With the development of technology in recent years, complex systems are developed rapidly, and more digital technologies and equipment are employed to ensure system safety and to increase production efficiency. However, these kinds of digital systems or equipment may increase complex interactions and interdependencies between subsystems and components (e.g., technical-human-organizational factors) (Sun et al., 2021; Zinetullina et al., 2021). Besides, this type of change may lead to new risks and challenges in the process industries. For example, once a fault occurs in one (or some) components, due to the strong interdependence between components, the fault will be propagated to the downstream nodes with a certain probability, which may gradually lead to the failure of the entire system (Wu et al., 2021).

With the introduction and development of digital technology in the process industries, the production process is almost entirely automated. The internal components of these systems are usually linked to each other. It is well known that when one component of the system fails, a cascade failure occurs, which in turn causes other components of the system to fail. As a result, the performance of the entire system degrades. Faults caused by cyber-attack or components failure (e.g., pump, sensor, controller, etc.) in process systems have gradually increased (Zhou et al., 2021). To enhance system safety, it is necessary to prevent accidents and deal with daily faults or disturbances timely to maintain system safety and production continuity. However, due to human errors, some faults are not undetected by operators or managers in time. For example, the failure of critical high-level alarm (LAH-5102) went undetected, which led to the fire and explosion accident at BP's refinery in Texas (CSB, 2007). Besides, to ensure the continuity of production and avoid production losses due to the shutdown of the unit or system, managers prefer to deal with faults online rather than use the Stop Work Authority (CSB, 2014). Under these two situations, faults may propagate to

* Corresponding authors.
E-mail addresses: sunhao_upc@outlook.com (H. Sun), wanghaiqing@upc.edu.cn (H. Wang), m.yang-1@tudelft.nl (M. Yang).

https://doi.org/10.1016/j.ssci.2023.106375
Received 23 August 2021; Received in revised form 21 July 2023; Accepted 2 November 2023
Available online 19 November 2023

downstream nodes with a certain probability, leading to faults propagation and accidents eventually (Wu et al., 2021). For example, in the accident that took place at the Chevron refinery, workers and managers found leaks in the 4-sidecut pipeline (i.e., faults). Before the pipeline leak occurred, the maintenance team did not conduct a full inspection of the pipeline as recommended. Besides, based on the local inspection results, they determined that only a small point leak had occurred in the pipeline. Therefore, instead of shutting down the system, they chose to deal with the leaks online to avoid production losses. This poor judgment and decision making led to a fire accident eventually, as the fault propagation and risk accumulated (CSB, 2014).

Peer researchers made significant contributions to assess the dynamic risk of a process system (Khan et al., 2020; Zhang et al., 2018; Ding et al., 2020; Hu et al., 2010; Zhu et al., 2021; Zhao et al., 2020; He et al., 2018). Because BN can handle uncertain information and its flexible modeling method, it is widely used in the field of risk assessment. Tong et al. (2020) proposed a method based on Dynamic Bayesian network (DBN) to measure the resilience of process systems. Zinetullina et al. (2021) integrated Functional Resonance Analysis Method (FRAM) and DBN to assess the resilience of process systems. Khakzad (2015) proposed a methodology based on DBN to model both the spatial and temporal evolutions of domino effects and quantify the most probable sequence of accidents in a potential domino effect. Khakzad et al. (2015) used an event tree to investigate the dynamic evolution of fire protection systems and developed a DBN to assess the temporal changes and influence on domino effects. Cai et al. (2018) used DBN to consider the performance and time-related properties to measure the resilience of engineering systems. Guo et al. (2021) proposed a novel fuzzy dynamic Bayesian network (FDBN) to enhance the ability of dynamic risk assessment (DRA) methods to quantify uncertainties caused by incorrect or insufficient data. Although the works described above show the significant contributions on dynamic risk assessment of process system, little attention has been paid to how to model the system systematically and how to assess the risk accumulation process considering two different engineering situations (i.e., fault is not processed, and fault is processed online) considering the digital age context. For digitalized process systems, interaction and interdependence of components and information feedback are essential factors to ensure system safety. They form a closed-loop within a process system. Bayesian network (BN) cannot model this closed-loop network because it is a directed acyclic network. In other words, BN cannot be employed to model complex or digital systems because it cannot take into account the interaction between components and the impact of information feedback on the system.

System-theoretic accident model and process (STAMP) can be a potential solution. It views safety as a control problem. Safety is managed by a control structure embedded in an adaptive socio-technical system (Leveson, 2004). In STAMP, the safety goal is to impose safety constraints on the system to sustain it in a normal state. STAMP has been proven to be a useful way to analyze safety in a highly complex system, particularly a process system, and is widely used in various fields (Altabbakh et al., 2014; Woolley et al., 2020; Yousefi and Hernandez, 2020; Zhang et al., 2021; Fu et al., 2020; Ouyang et al., 2010; Abdulkhaleq et al., 2015; Sultana et al., 2019; Goncalves Filho et al., 2019; Stanton et al., 2019; Castilho et al., 2018). Systematically modeling a system is the basis for accurate risk assessment. If the system cannot be accurately modeled, the risk assessment result cannot represent the actual risk of the system. The STAMP-based dynamic risk assessment model can more rigorously analyze the nonlinear interdependence, interaction, and feedback between complex technical-human-organizational factors and better reflect the real-world situation of a process system.

A quantitative method is proposed in this paper to model the process of risk accumulation, which consists of two cascading failure propagation models (CFPM). Cascading failure refers to when a node of the system fails, and the fault may propagate to downstream nodes and cause them to fail. Most studies about cascading failure focus on the power system, industrial internet platform, critical infrastructure networks (Yang et al., 2021; Li et al., 2020; Duan et al., 2018). Two novel CFPMs and the mechanism of failure propagation under two different engineering situations (i.e., fault is ignored, and fault is processed online) are proposed and described in this paper to assess the process of risk accumulation. It can help workers and managers to determine when the unit or system should be shut down to prevent accidents.

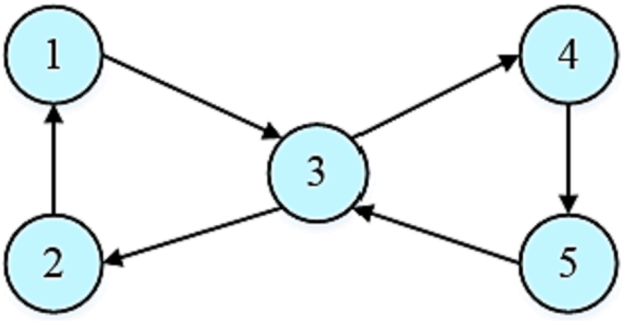

Fig. 1. Interdependence of nodes in a process system.

The present study aims to develop a dynamic quantitative risk assessment method for chemical process systems considering the process of risk accumulation caused by digital technologies and equipment based on system theory and CFPM. Firstly, STAMP is used to model the system systematically to develop a network model. After this, two CFPMs are proposed to assess the risk accumulation of the system under two different engineering situations. To the best of the authors' knowledge, it is the first time to integrate STAMP and CFPM to assess the risk accumulation of a chemical process system.

The remaining parts of this paper are organized as follows. The preliminaries are presented in Section 2. A brief description of the proposed method, including STAMP modelling, the categories of real engineering situations, the process and mechanism of risk accumulation, and how to assess the dynamic risk of the system, is shown in Section 3. The case study is presented in Section 4. The comparison with DBN and the determination of the shutdown time are discussed in Section 5. Finally, conclusions are drawn in Section 6.

2. Preliminaries

2.1. The influence of digital technology in the process industries

Digitalization is defined as the integration of digital technologies in process operations for greater efficiency and increased product quality (Khan et al., 2021). Digitization often means integrating information such as human judgment and decisions, empirical data, and detector data to help systems operate safely, improve efficiency and productivity, and respond flexibly to change. A production process within the process industry is a complex system with multiple constraints, multiple goals, and a complex hierarchical structure. It integrates information flow, material flow, and energy flow. With complex physical and chemical reactions, there are significant mutations and uncertainties. Due to the hazardous nature of these processes, high safety and reliability requirements are in place for the process industry.

The benefits of digital technology are reflected by:

(1) The generation of digital operational data and;
(2) The use of software-based automation to replace manual process operations. Thus, data can be automatically collected for effective process monitoring to ensure system safety (Khan et al., 2021).

However, digital technology has brought some safety issues while improving the production efficiency of process systems, which are

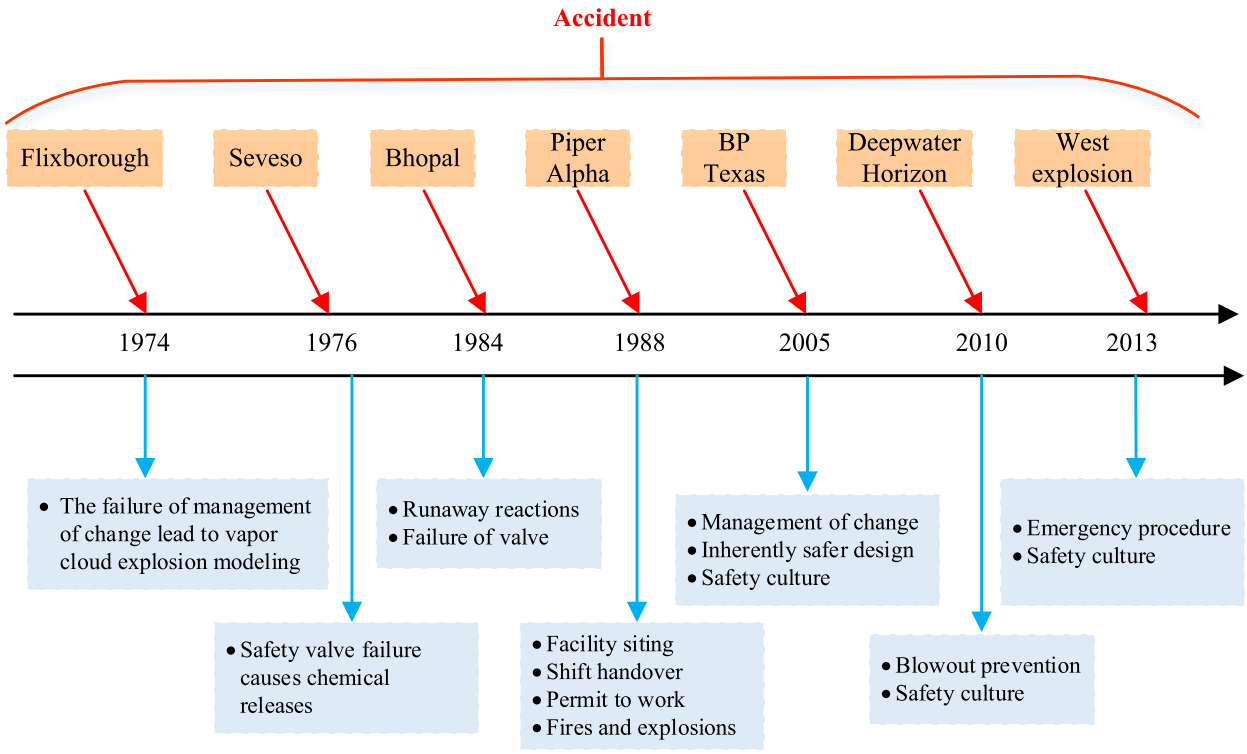

Fig. 2. The cases of accident in chemical process system.

described as following:

(1) The use of automation increases the interdependencies and interactions of components in a process system. This makes the process system more complex. A closed-loop may form. Fig. 1 gives an example of such a closed-loop. This type of network brings difficulties to traditional risk analysis methods. When a node fails, the fault will propagate to downstream nodes with some probability. Since the network is a closed-loop network, the fault may propagate to every node in the system and cause system failure, increasing system risk.

(2) Digitization brings with it the opportunity to generate and collect digital operational data, reducing human manipulation and enabling effective process monitoring and control to ensure safety. At the same time, digitization increases the complexity of human–computer interaction, which brings new research and practical problems (Pasman et al., 2022). For example, when the detector is faulty, the wrong information will feedback and affect human operation and judgment, resulting in the fault constantly propagating to neighboring nodes, which may eventually lead to accidents. Once the equipment or instruments fail, the fault will propagate to workers, leading to wrong reading or decision. For example, suppose the liquid level gauge of a tank fails. In that case, it may lead to erroneous reading, which may cause an incorrect decision and operation, and consequently, an overflow accident may occur. A well-known example is the Buncefield oil storage station accident that occurred on December 11, 2005. The main reason for the overfilling of gasoline tanks was the failure of the automatic tank metering system (Paltrinieri et al., 2012). More examples are shown in Section 2.2.

Due to the increasing complexity of the digital system, the components are interrelated and affect each other. Once one or some components fail, the system will be seriously affected. As a result, digital systems are more attractive to cyberattacks and deliberate attacks and vulnerable to component failure (Zhou et al., 2021; Varadharajan and Bajpai, 2023). Therefore, detecting and dealing with faults promptly, understanding the fault propagation mechanism, and cutting off the fault propagation path is essential to prevent catastrophic accidents in any digitalized process system.

2.2. *Review of past accidents*

On March 23, 2005, a severe fire and explosion occurred in the isomerization unit of BP's refinery in Texas, USA. Before the accident, the operator directly turned on the pump to send combustible materials into the fractionation tower without following the procedures to check the meter of the tower. The operator did not correctly read the liquid level data, and the critical high-level alarm (LAH-5102) also failed. Under these circumstances, the operator continued to feed the tower with the material until the high liquid level alarm (LT-5100) of the liquid level indicator sounded an alarm when the tower was full, and the material in the tower overflowed into pipelines at the top of the tower. When the pipelines at the top of the tower were filled with liquid, the pressure at the inlet of the top condenser rapidly rose from 144.69 kPa to 440.96 kPa, and the three top relief valves were opened to discharge the material into the blowdown drum and the chimney. The blowdown drum and the chimney overflowed one after another, and a large amount of liquid gushed out from the top of the chimney like a fountain. These volatile liquids formed a combustible gas cloud when they reach the ground. The spreading vapor cloud was ignited by a truck that had not stalled, and the flame spread rapidly, followed by a series of explosions in the installation area. The accident resulted in 15 deaths and 170 injuries. The specific accident investigation can be seen in CSB (2007).

On Sunday, December 11, 2005, a Vapour Cloud Explosion accident happened at Buncefield oil storage depot in the UK. The main event of this accident is overfilling of tank 912. In the early morning of December 11, 2005, the automatic tank gauging (ATG) system fitted on the tank stuck, indicating that the tank was 2/3 full level. Besides, the safety system to prevent oil spills (Independent High-Level Switch) had been inadvertently turned off after a test. Thus, the tank was overfilled. Approximately 300 tons of gasoline were released from the tank, and 10

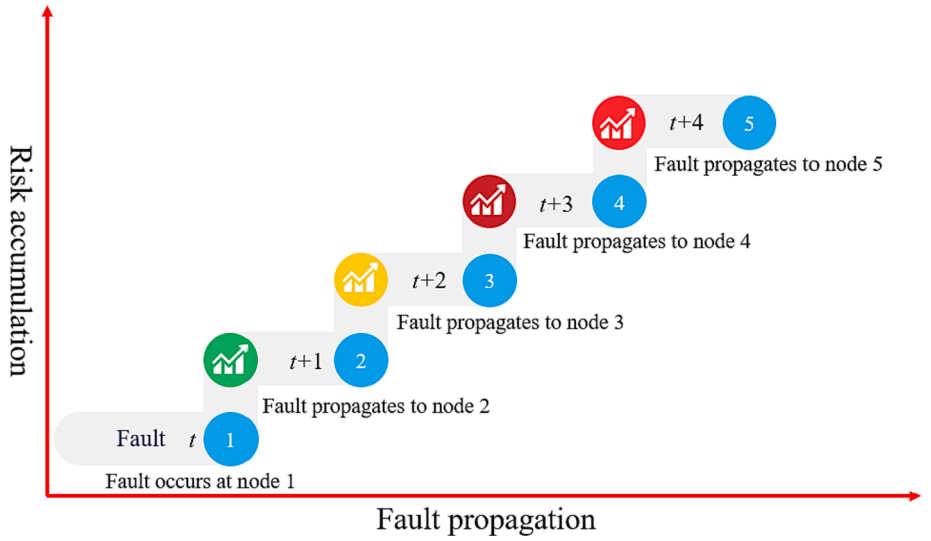

Fig. 3. The process of fault propagation and risk accumulation.

% of it was converted into vapor mixed with cold air. Under windless conditions, its concentration was sufficient to support combustion (Paltrinieri et al., 2012; HSE, 2008; HSE, 2011).

On November 28, 2018, a major deflagration accident occurred in China National Chemical Corporation Shenghua Chemical Company, Zhangjiakou City, Hebei Province (Department of Emergency Management of Hebei Province, 2019). The direct cause of the accident was that the #1 vinyl chloride gasometer in the PVC workshop of Shenghua Chemical Company was not overhauled according to regulations for a long time. Before the accident, the vinyl chloride gasometer was stuck, tilted, and leaked, and the compressor inlet pressure was reduced. Due to negligence, the gasometer was not found to be stuck, and the compressor return was increased as in normal operation. The amount of gas entering the gas tank was increased. The vinyl chloride broke through the annular water seal, causing a leakage accident and spreading outside the plant area. After encountering an ignition source, deflagration occurred. The accident caused 24 deaths and 21 injuries.

More accidents can be seen in Fig. 2, e.g., explosion accident in Flixborough (Mannan et al., 2012), Seveso accident (Hay, 1977), Bhopal accident (Mannan et al., 2005), Piper Alpha accident (Mannan, 2005), etc. According to these accident investigations, it can be seen that even though various safety methods are used to ensure system safety, failures cannot be completely eliminated. In the Chevron refinery accident, workers found the precursor or events of the accident, the managers and operators still chose online maintenance rather than shut down the unit (CSB, 2014). The results of accident investigations proved that the risk accumulates over time until an accident occurs. Therefore, it is meaningful to assess the risk accumulation process to prevent accidents and provide support for decision-making. In addition, the real-time dynamic risk profile can help the operator to determine when maintenance measures should be taken or when the unit needs to be shut down.

2.3. Two engineering situations of fault propagation in process system

(1) Faults are not processed

Fault is a state in which a system or component cannot perform a specified function, such as equipment fault, instrument fault, human error, etc. In other words, fault refers to the fault of some components in the system and leads to the deterioration of the function of the entire system. When a fault occurs in the system, it will affect the function of a component. Due to the characteristics of the complex system (i.e., closed-loop system), the downstream node will be affected by the failure of upstream component over time. Thus, the system function state will be reduced over time. In the real-world production process, faults are often ignored due to technical or human factors. Intentional negligence includes equipment or workers that have discovered and reported faults, but managers believed that the faults would not impact the system and thus chose to ignore them. It is also possible that workers noticed the faults but did not deliberately report back to the manager or take action because they thought it was not necessary. Unintentional negligence includes failure to feedback faults to the control system in time due to equipment failure (e.g., the sensor fails), failure to detect faults in time (due to negligence of the operator), lack of experience or knowledge of the operator, and failure to handle faults in time due to unattended control in the control room.

These failures and negligence will lead to faults that will not be handled in time, which will lead to the faults propagating downstream. Since no maintenance actions are taken, the risk of the system will gradually accumulate as the fault propagation, which may eventually lead to accidents. In this case, the specific process and mechanism of fault propagation can be seen in Fig. 6 in Section 3.2.1.

(2) Faults are processed online (i.e., without shutting down the system)

Due to the high daily production volume of the process system, to avoid economic losses caused by the shut-down of a system or a unit, workers and managers tend to choose online processing when they find faults. In other words, workers and managers are unwilling to use the Stop Work Authority (CSB, 2014). Even if maintenance measures are taken in time, the faults may propagate to downstream nodes because the unit or system is not shut down. This probability of fault propagation depends on the maintenance coefficient M described in Section 3.2.2. The mechanism and process of fault propagation under this engineering condition are shown in Fig. 7 in Section 3.2.2.

To measure the risk accumulation of these two different engineering conditions, the system is modeled as a discrete dynamical system, which can be used to determine a series of time-varying sequences of system states (Wu et al., 2021). For example, the fault occurs at node 1 at time t, and it will propagate to downstream nodes at the next time (i.e., $t + 1$). The schematic diagram of fault propagation and risk accumulation is shown in Fig. 3, and the specific process and mechanism are discussed in Section 3.2.

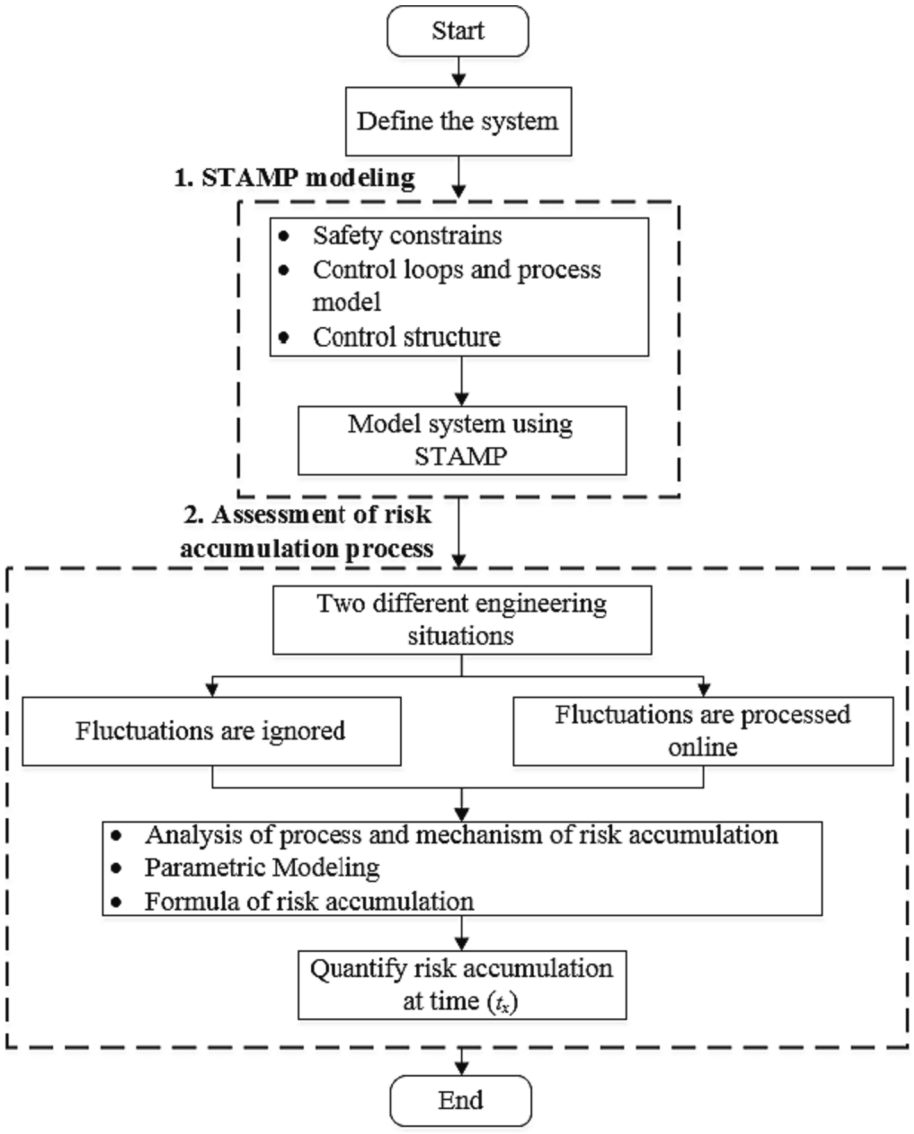

Fig. 4. The proposed methodology for assessing the system resilience.

3. The proposed methodology

The methodology developed in this section serves to assess risk accumulation when a fault is ignored or processed online, and includes two main parts, namely, modeling the system using the STAMP approach and measuring the process of risk accumulation based on a cascading failure model. Firstly, the safety constraints, control loops, process model, and control structure should be identified to model the system. Afterwards, the parametric modeling and the risk accumulation formula should be determined to assess the process of risk accumulation. The following section describes the main steps of the proposed method. The specific process is shown in Fig. 4.

3.1. STAMP modeling

Technology is moving forward, and process systems are increasingly becoming automated, interdependent, and complex. The role of human beings in the system is changing, so we should start from the perspective of the system to deal with safety from component reliability to system thinking.

STAMP views complex systems as combinations of interdependent subsystems and components, keeping a dynamic equilibrium state through information feedback loops and control (Leveson, 2004). Safety is regarded as an emergent system property by STAMP. The unwanted interactions between components and subsystems, which violate the safety constraints of a system, are the leading causes of accidents (Sultana et al., 2019). Three main concepts consist of STAMP: safety constraints, control loops, process models, and control structure (Yousefi and Hernandez, 2020).

(1) In STAMP, system safety is regarded as a control problem. Safety constraints are essential for a system to ensure it operates within a safe range. The occurrence of major accidents is due to component failure or human error and the ineffective implementation of safety constraints of the system. In other words, accidents occur when there are no safety constraints or the safety constraints fail to control the hazards. There are four different types of unsafe 'safety constraints' or control actions (UCAs) defined by STPA as following (Leveson, 2004): i) control actions required for safety are not provided, ii) unsafe control actions occur, iii) potential control actions are provided at the wrong time (too early, too late, or in the wrong order), and iv) the demanded control actions are stopped too soon or applied too long.

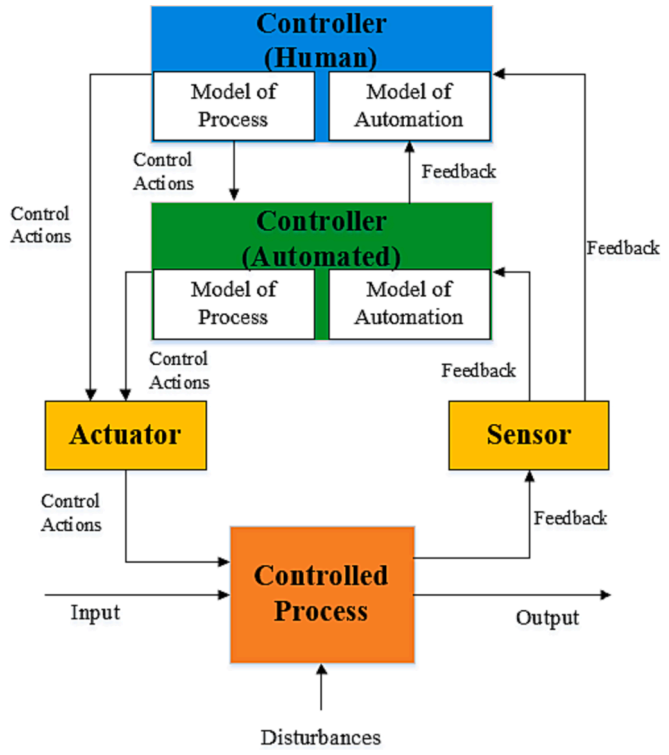

Fig. 5. Basic control loop of STAMP (Leveson, 2004).

(2) Control loops are vital parts of system safety. The control actions and information feedback in the control loops are critical to ensure system safety. There are five main components in control loops: controller, process model, actuator, controlled process, and sensor. The role of the process model is to determine the control actions according to the information feedback from sensors to ensure system safety. The typical control loop is shown in Fig. 5.

(3) Control loops exist in every level of control structure. In system theory, the system is regarded as a hierarchical structure. In the control structure, upper-level components control lower-level components through safety constraints or control actions (Leveson, 2004). In the light of the control structure, the roles and responsibilities of each element of STAMP can be determined. It helps engineers identify potential hazards and interactions between subsystems and components systematically.

3.2. Quantification of the risk accumulation process

STAMP is an effective method to model the system. However, it can only analyze the system safety qualitatively. Therefore, a quantitative approach should be proposed to calculate the process of risk accumulation to identify when the unit or system should be shut down to prevent an accident. The following sub-sections describe the quantitative models developed for two general operational scenarios of a process system.

3.2.1. CFPM when fault is not processed (without maintenance)

The state of the system often fluctuates during the production process. Sometimes, due to managers or workers believing that some faults will not affect the system, faults are ignored. However, small faults will gradually transmit downstream, and the risks accumulate over time, which may eventually cause accidents. To measure this kind of risk, a quantitative method is proposed based on a cascading failure model.

We define that failure probability of node i is between 0 and 1, and 0 indicates the node is at a normal state and 1 means the node is down. The failures propagation has some time lags in a process system. Thus, in the model, nodes affect their downstream nodes with some time delays and probabilities when the nodes fail or are attacked by a human or hacker (cyber-attack) (Jing et al., 2019). Therefore, we model a system as a discrete dynamical system, which can be used to determine a series of time-varying sequences of system states (Wu et al., 2021). Fig. 6 provides an example. Node i fails at time t, and at the next moment $(t+1)$ the failure will propagate to node j. The rest propagates in the same manner. It is worth noting that node j will transmit failure to downstream node k at time $t+2$. At the same time, it will be affected by itself.

Due to the disruption at node i, the failure probability of node i is assumed as 1. The probability of failure propagation depends on the weight of the directed edge (i.e., the conditional probability $P(j|i)$ in Fig. 4). Therefore, the failure probability of node j at time $t+1$ is:

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

where $P_i(t)$ indicates the failure probability of node i at time t, $P(j|i)$ presents the conditional probability of node i failing causing node j to fail. We assume that the conditional probability $P(j|i)$ does not change over time in this paper.

At time t + 2, node j is not only affected by upstream node i, but also affected by.

its own state degradation. At this time, the failure probability of node j at time $t+2$ can be expressed as Eq. (2), and the rest can be calculated in the same manner.

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

where $P_j(F_{t+2}|F_{t+1})$ represents the conditional probability that node j fails at time $t+2$ when it fails at time $t+1$; $P_j(F_{t+2}|S_{t+1})$ indicates the probability of node j failing at time t + 2 if it does not fail at time $t+1$.

Duo to maintenance measures are not conducted in this practical condition, the $P_j(F_{t+2}|F_{t+1})$ eques to 1. Therefore, Eq. (2) can be represented by Eq. (3):

$$P_j(t+2) = P_j(t+1) + [1 - P_j(t+1)] \times P_j(F_{t+2}|S_{t+1}) \tag{3}$$

Therefore, we can conclude that the failure probability of node j when it is affected by node i at time t_x ($t_x \geq 2$) is:

$$P_j(t_x) = P_j(t_x - 1) + [1 - P_j(t_x - 1)] \times P_j(F_{t_x}|S_{t_x-1}) \tag{4}$$

When the node j is jointly affected by two or more nodes. If the failure of any of these nodes will cause the state change of node j, it is said that these upstream nodes form a logical OR gate relationship with node j. The failure probability can be calculated by Eq. (5) (adapted from Wu et al., 2021).

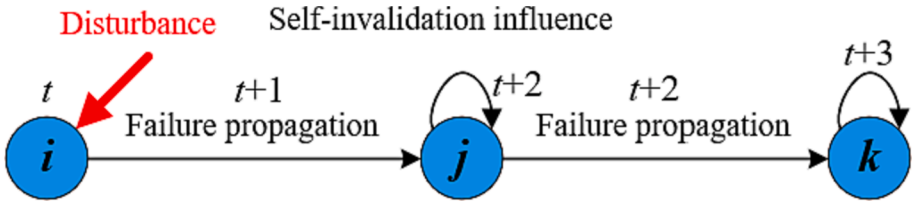

Fig. 6. The mechanism of risk accumulation when fault is ignored.

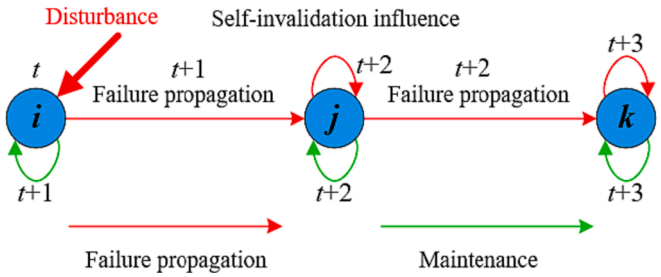

Fig. 7. The mechanism of risk accumulation when a fault is processed online.

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

where u denotes a node that affects node j, n is the number of nodes that affected node j. Note that node j can be regarded as a failed node when $P_j(t_x) = 1$.

It is worth noting that there is another situation, that is, when two nodes both fail at the same time, it will affect the downstream nodes, similar to the AND gate in the fault tree. For example, when feeding materials to the reactor, if the primary pump fails, the standby pump can be switched to maintain the normal operation of the system. However, when the two pumps fail at the same time, it will affect the system. In this case, Eq. (5) can be changed to Eq. (6) (adapted from Wu et al., 2021):

$$P_j(t_x) = P_j(F_{t_x}|S_{t_x-1}) + \left[\prod_{u=1}^{n}(P_u(t_x - 1) \times P(j|u))\right] \times [1 - P_j(F_{t_x}|S_{t_x-1})] \quad (6)$$

According to Eq. (4), Eq. (5) and Eq. (6), the failure probability of all nodes at a discrete time can be measured. On this basis, the change of system state caused by fault propagation can be determined by Eq. (7).

$$R_S(t) = 1 - \frac{\sum_{a=1}^{m} f_a \cdot P_a(t)}{\sum_{a=1}^{m} f_a} \quad (7)$$

where R_s indicates the remaining performance of the system, m is the number of nodes in the system, t represents the discrete time, which satisfies $0 \le t \le t_f$, t_f is the failure time of the system, f_a indicates the weight of node a, which can be determined by Eq. (8).

$$f_a = \frac{d_a}{m} \quad (8)$$

where d_a represents the number of nodes connected to node a, m is the number of nodes in the system. It is worth noting that the more important the node, the greater the impact of its state on the system.

3.2.2. CFPM when fault is processed online

The previous section describes one of the practical engineering situations of a process system. However, there is another engineering situation. The accident investigation reports found that to avoid production losses caused by closing the unit, workers or managers are sometimes unwilling to shut down the unit (WSB, 2014). To measure this kind of risk accumulation process, another quantitative approach is proposed. The specific process of fault propagation in this situation can be seen in Fig. 7.

The process of fault propagation is the same as the previous one, which is described in section 3.2.1. Due to managers or workers deciding to maintain the abnormal nodes without shutting down the system, these kinds of nodes will recover the lost state with a certain probability. Therefore, the failure probability of node j at time $t + 2$ can be expressed as Eq. (9).

$$P_j(t+2) = P_j(t+1) \times P_j(F_{t+2}|F_{t+1}) + [1 - P_j(t+1)] \times P_j(F_{t+2}|S_{t+1}) \quad (9)$$

where $P_j(F_{t+2}|F_{t+1})$ represents the conditional probability that node j fails at time $t + 2$ when it fails at time $t + 1$; $P_j(F_{t+2}|S_{t+1})$ indicates the

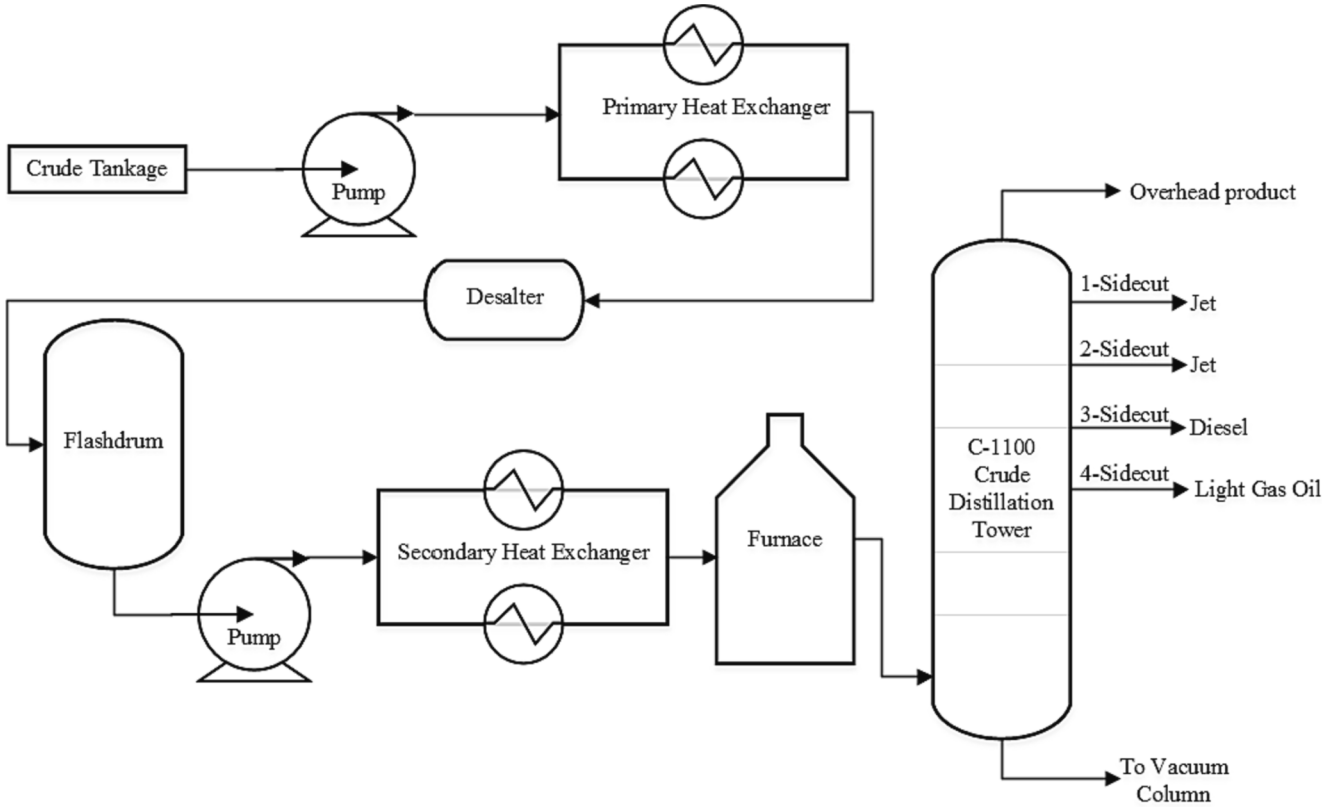

Fig. 8. Schematic diagram of the Chevron Richmond refinery crude unit.

probability of node j failing at time t + 2 if it does not fail at time $t + 1$.

Note that $P_j(t + 2)$ may be less than 0 in this case. Therefore, we define that when $P_j(t + 2)$ is equal to 0, node j can be regarded as a normal state, and its failure probability is 0.

The failure probability of node j when it is affected by node i at time t_x ($t_x \geq 2$) is:

$$P_j(t_x) = P_j(t_x - 1) \times P_j(F_{t_x}|F_{t_x-1}) + [1 - P_j(t_x - 1)] \times P_j(F_{t_x}|S_{t_x-1}) \quad (10)$$

When the node j is jointly affected by two or more nodes, its failure probability can be described as Eq. (11).

$$P_j(t_x) = P_j(F_{t_x}|F_{t_x-1}) + \prod_{u=1}^{n}(1 - P_u(t_x - 1) \times P(j|u)) \times [P_j(F_{t_x}|S_{t_x-1}) - P_j(F_{t_x}|F_{t_x-1})] \quad (11)$$

When two nodes both fail at the same time, it will affect the downstream nodes. Similar to the AND gate in the fault tree. In this case, Eq. (11) can be changed to Eq. (12):

$$P_j(t_x) = P_j(F_{t_x}|S_{t_x-1}) + \left[\prod_{u=1}^{n}(P_u(t_x - 1) \times P(j|u))\right] \times [P_j(F_{t_x}|F_{t_x-1}) - P_j(F_{t_x}|S_{t_x-1})] \quad (12)$$

According to the Eq. (10), Eq. (11) and Eq. (12), the failure probability of each node in the system can be quantified. The remaining performance of the system at each time point can be calculated by Eq. (7). Therefore, the process of fault propagation can be measured.

4. Case study

4.1. Descriptions of the case

On August 6, 2012, a disastrous fire accident which was caused by a pipe rupture in a crude distillation unit in the "Chevron Richmond refinery" occurred. The accident originated from one of many process streams called the "4-side cut" leaving the Richmond refinery's C- 1100 Crude unit atmospheric column (Adedigba et al., 2018), which caused flammable light oil released at the rate of 10,800 barrels per day (CSB, 2014). The crude oil stored in the crude tankage was pumped to a primary heat exchanger for heating. The salt content of crude oil can cause great and harmful effects on the processing of crude oil, thus, the desalter is used to remove corrosive salts, solids and water. Then the volatile light hydrocarbons were removed through the flashdrum. Afterwards, the materials were pumped to the secondary heat exchanger and the furnace for heating. Finally, the oil is pre-heated and enters the C-1100 Crude Unit Atmospheric Column (Crude Column) at approximately 675 degrees Fahrenheit (°F). Details about the Richmond refinery accident can be found in the CSB investigation report (CSB, 2014). The process of the Chevron Richmond refinery crude unit and its associated upstream process is used to illustrate the proposed methodology, as shown in Fig. 8.

4.2. STAMP modeling for Richmond refinery crude unit

The process of the Chevron Richmond refinery crude unit and its associated upstream process is a typical complex system. It is essential to analyze system safety within a system context to prevent system failure and acquire a comprehensive understanding of the role of the components, its interactions, and its interdependencies. Before assessing the process of risk accumulation of the system, it is necessary to model the system. In this case, STPA is used to identify system hazards, and STAMP is used to model the system.

Identifying system boundaries is the first step to model the system. The process of the Chevron Richmond refinery crude unit and its associated upstream process is selected as the boundary of the system, which is shown in Fig. 8. The analysis aims to understand better the mechanism and model of the process of risk accumulation.

Table 1
The facilities' roles of the Richmond refinery crude unit system.

Facility	Roles
Pump	Pumps the crude oil in oil tank to primary heat exchanger
Primary heat exchanger	Preheat the crude oil and send it to the desalter
Desalter	Removes corrosive salts, solids and water in crude oil
Flashdrum	Removes the volatile light hydrocarbons in crude oil
Secondary heat exchanger	Preheat the crude oil and send it to the furnace
Furnace	The crude oil is heated to a specific temperature
Distillation tower	The crude column separates through distillation various hydrocarbon component mixtures in the crude feed, creating multiple streams coming off the column with different boiling points.
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, control the temperature and pressure
Controllers	Reduces or controls flow rate, temperature, pressure by the automatic controller (DCS or SIS)

Before developing the system control structure, the first task is to determine the various equipment and their roles in the system. The main equipment of the above-mentioned process include pump, primary heat exchanger, desalter, flashdrum, secondary heat exchanger, furnace, and crude distillation tower. The controllers include site operators, indicators, alarms, and controllers for main variables (e.g., flow rate, temperature, pressure, level). The main task of controllers is to keep the variables in the process within the set value or certain range to ensure system safety. The specific equipment and their roles are shown in Table 1. According to the STPA and STAMP method, the control structure of the system is shown in Fig. 9.

Fig. 9 shows the control structure of the system, where the down arrows indicate control actions for applying safety constraints to the downstream nodes, and the down dashed arrows represent control actions from site operators applying safety constraints to the downstream nodes. Besides, the up dashed arrows represent feedback, which provides information on how the parameters in the system change over time and how effectively the control actions are performed.

The control relationships between components are shown in Fig. 9. However, the interactions and interdependencies between system equipment (e.g., pump, heat exchanger, desalter, flashdrum, etc.) are not well expressed. Due to the mutual influence between the equipment in the process system, the states of the upstream equipment in the system will affect the states of the downstream equipment. For example, when the desalter fails, it will affect the state of the flashdrum with a certain probability. Therefore, there are mutual influence relationships between the equipment of the system. The specific influences between equipment (i.e., node 6 to 13) of the system are discussed in section 4.3.

The operation and process parameters must be controlled and maintained within a safe range to ensure system safety. Besides, the potential unsafe control actions (UCAs) should be identified to prevent accidents. According to the system, all nodes (e.g., corporate, plant managers, controllers, actuators, and sensors) and their interactions should be considered. The UCAs can be divided into four categories, which have been discussed in Section 3.1 (Leveson, 2004). The specific UCAs, their causes, and safety constraints are shown in Table 2.

4.3. Quantification of the risk accumulation process

According to the STAMP model developed in Section 4.2 (i.e., Fig. 9), the network of the system can be extracted as Fig. 10. It is worth noting that a red arrow is added based on the STAMP model to represent the interdependence of equipment and to show the influence of upstream equipment on downstream equipment, which means that when the

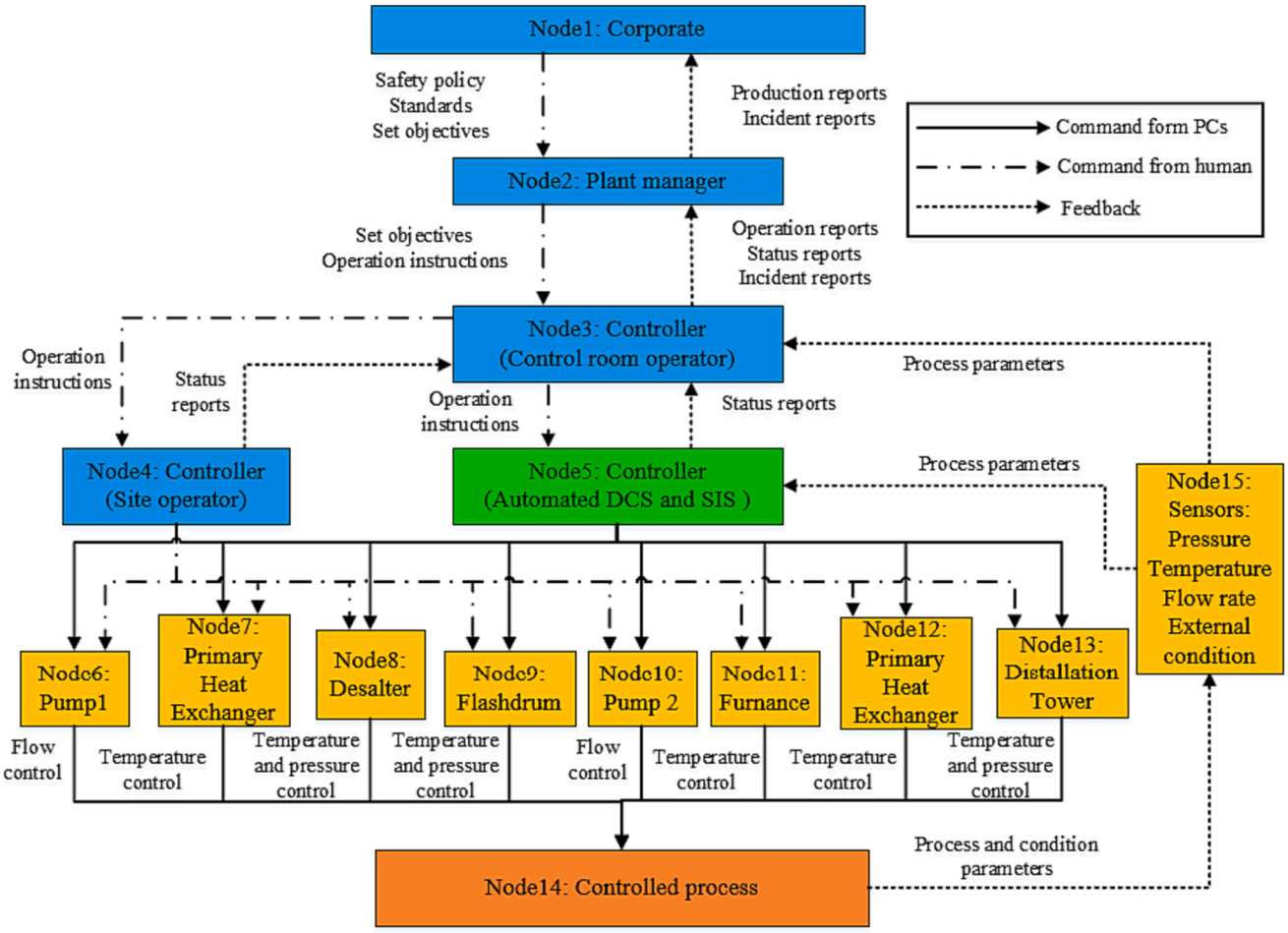

Fig. 9. Control structure of the Richmond refinery crude unit system.

upstream equipment fails, it may lead to a state change of downstream equipment with a specific probability.

According to Eq. (8) and Fig. 10, the parameters of the fault propagation process are determined and shown in Table 3. Specifically, node degree is represented by the number of nodes connected to the node. The f_a indicates weight of the node, which can be determined by Eq. (8). Due to the engineering situations being divided into two categories, the processes of risk accumulation are analyzed in two parts, which are discussed in Section 4.3.1 and Section 4.3.2.

4.3.1. CFPM when fault is not processed (without maintenance)

Sometimes, due to the intentional or unintentional negligence of managers and operators, the fault is ignored, which may lead to the fault propagating to downstream nodes. Subsequently, the fault can be propagated to all nodes of system, because STAMP is a closed-loop model. Faults are not processed, which means that no maintenance measure is taken to stop or mitigate this type of propagation. The system state will be reduced over time, and the system risk will be increased. In this case, we assume that the fault occurs at node 3. A non-dimensional time interval is used to demonstrate the proposed method, and time units do not refer to a specific problem set-up but serve as proof of concept.

Due to the interaction between components in the system, a node may be affected by two or more nodes. For example, in Fig. 10, node 3 is not only affected by node 2 but also by node 4, node 5, and node 15 (information feedback), which means that the child node of a node in the STAMP model may also be the parent node of the node (cyclic reinforcement). This illustrates the complex interaction and interdependence between nodes of the system. In other words, the proposed method not only considers the interaction between components but also considers the influence of information feedback on components. Therefore, the proposed mothed can accurately model complex systems and accurately calculate the risk accumulation process. This is the difference between the proposed method in this paper and other traditional methods, and it is also the advantage of the proposed method.

In the light of the proposed CFPM, when a fault is ignored in Section 3.2.1, the states of all nodes are determined by Eq. (4), Eq. (5), and Eq. (6). According to Eq. (7) and Table 3, the processes of fault propagation at different time are shown in Fig. 11.

It can be seen from Fig. 11 that, due to a fault is ignored (i.e., without maintenance), it is propagated to downstream nodes, leading to the system performance decreases rapidly over time. It is worth noting that when a fault propagates to the downstream node, the feedback from the downstream nodes will affect its upstream nodes and increase the failure probability of nodes. This is a vicious circle and exacerbates the process of fault propagation because STAMP is a closed-loop model. For example, a fault occurs on node 3 at time t, the fault will be propagated to node 4 and node 5 at $t+1$. At time $t+2$, fault will be propagated from nodes 4 and 5 to downstream nodes (i.e., 6, 7, 8, etc.), and nodes 4 and 5 will be affected by themselves at the same time. Besides, the error feedback of node 15 will affect node 5 at time $t+5$, and the rest can be done in the same manner. Therefore, the system risk may reach a high value in a short time.

Note that the engineering meaning of this method is to provide a dynamic system performance profile, and the time to shut down the system can be determined according to the minimum acceptable remaining performance (MARP) of the system to prevent accidents. For example, if the MARP is 0.50, the system must be repaired before $t+2$ to

Table 2
The UCAs for Richmond refinery crude unit system.

Category	UCAs	Causal factors	Safety constraints
Control action is not provided	Sign of the high pressure in the system is not detected	Pressure indicator and alarm fail	Inspection and maintenance
	Sign of the high temperature in the system is not detected	Temperature indicator and alarm fail	Inspection and maintenance
	Sign of the high/ low flow rate in the system is not detected	Flow rate indicator and alarm fail	Inspection and maintenance
	Failure of system equipment is not detected	Operators lack of skill and experience	Safety training
Control action is unsafe	The detected pressure in the system is wrong	Pressure indicators fail, or operators misread pressure	Inspection and maintenance, training
	The detected temperature in the system is wrong	Pressure indicators fail, or operators misread the temperature	Inspection and maintenance, training
	The detected flow rate in the system is wrong	Flow rate indicators fail, or operators misread flow rate	Inspection and maintenance, training
Control action occurs too early or too late	Operators do not take action in time	Operators lack of skill and experience	Safety training
	The command from the control room is too early or too late	Operators in control room lack skill and experience	Safety training
Control action is stopped too soon or applied too long	The control actions of the pump or heat exchanger are stopped too soon or too long.	Operators at control room lack of skill and experience; Operators lack of skill and experience; DCS or SIS fails	Safety training; Inspection and maintenance

help the system recover the performance.

4.3.2. *CFPM when fault is processed online*

Repair measures can reduce the speed and degree of fault propagation. However, "repair" is a process that needs some time to carry out. In this period, a fault will be propagated to downstream nodes with a low probability. Consequently, the fault can be propagated to all nodes of the system because STAMP is a type of closed-loop model. Finally, the system state will be restored to the normal state with repair online. Due to the limitations of space, ten time intervals are used to illustrate the proposed method.

According to the proposed CFPM, when a fault is processed online in Section 3.2.2, the states of all nodes in the system are calculated by Eq. (10), Eq. (11) and Eq. (12). The process of fault propagation is determined in Eq. (7), and the results are shown in Fig. 12.

It can be seen from Fig. 12, although the fault is processed online (i.e., external repair), the fault is propagated to downstream nodes, which leads to the system risk increasing at the first time. Then, the system performance reaches the minimum value (0.63) at time $t + 2$. Afterwards, as the maintenance continues, the state of nodes in the system begins to recover. The speed of recovery depends on the degree of repair.

Note that the engineering meaning of this model is to provide a dynamic performance profile under the situation of repair online. Besides, it can help operators determine when to repair the system according to a pre-defined the minimum acceptable remaining performance (MARP) of the system to ensure system safety. It can also avoid the unnecessary shutdown of system to ensure the continuous

Table 3
The parameters of fault propagation for Richmond refinery crude unit system.

Node	Degree	f_a
1	1	0.067
2	2	0.133
3	4	0.267
4	9	0.600
5	10	0.667
6	4	0.267
7	5	0.333
8	5	0.333
9	5	0.333
10	5	0.333
11	5	0.333
12	5	0.333
13	4	0.267
14	9	0.600
15	3	0.200

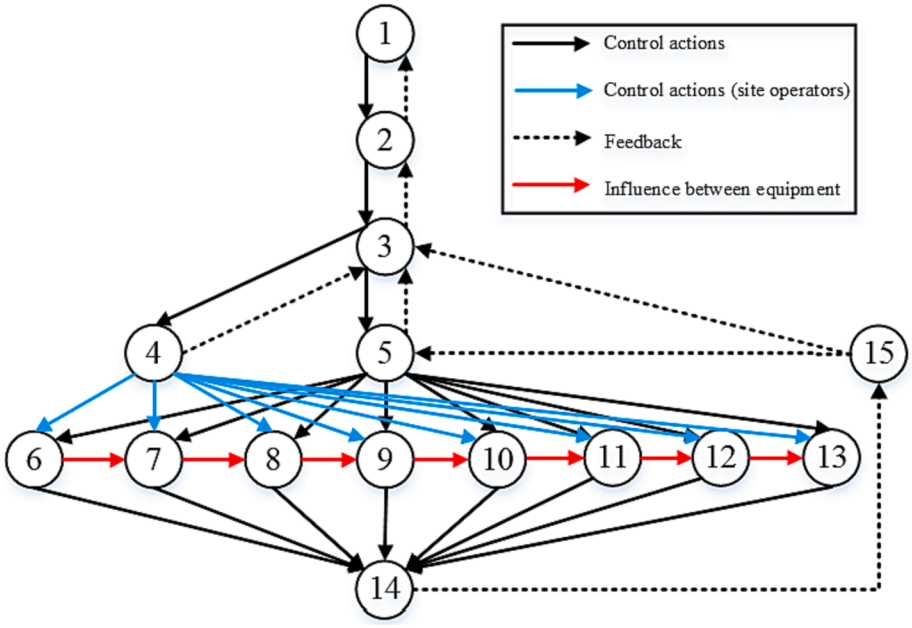

Fig. 10. Network diagram extracted from Fig. 8.

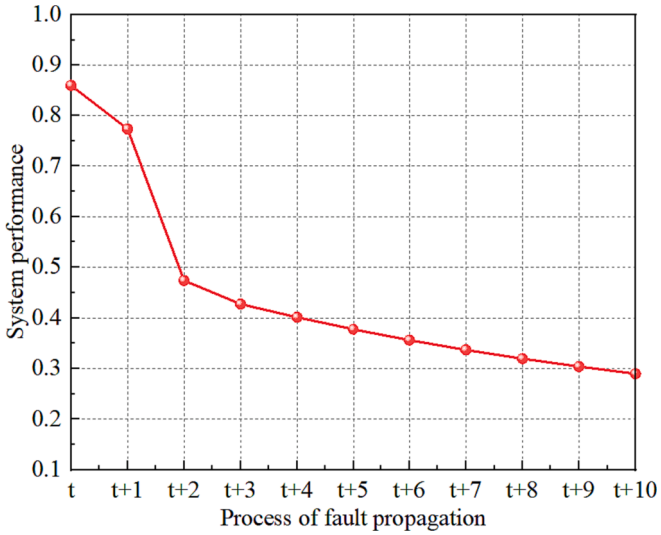

Fig. 11. System performance changes over time when a fault is not processed.

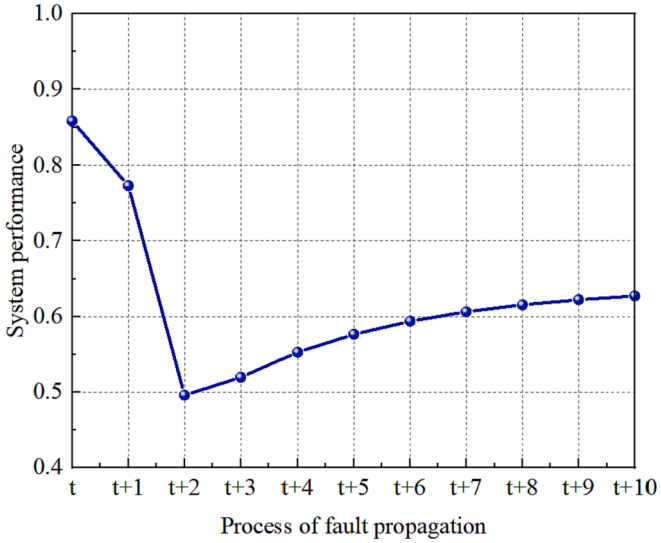

Fig. 12. System performance changes over time when fault is processed online.

production of the system or unit. For example, the MARP is assumed as 0.50. This situation does not require downtime for maintenance. In other words, online repair measures can be taken to deal with the fault propagation process in this condition because of the minimum system performance is larger than MARP in this condition.

By comparing Fig. 11 and Fig. 12, it can be seen that timely repair has a great impact on system safety. If the fault is ignored, the system risk will increase rapidly, possibly leading to major accidents. For complex systems, the stronger the dependence between components, the greater the probability of the fault propagating to downstream nodes, and the faster the risk accumulates. When external maintenance or emergency actions are taken, the propagation of faults and the accumulation of risks can be controlled to a certain degree, which depends on maintenance. The impacts on system performance was investigated when different time steps are delayed to process faults online, which are shown in Fig. 13. It can be seen from Fig. 13, handling fault nodes in a timely manner can reduce system performance loss and speed up system performance recovery.

Since the interdependence cannot be reduced in a complex system, the system safety can be enhanced from two aspects: i) increasing the

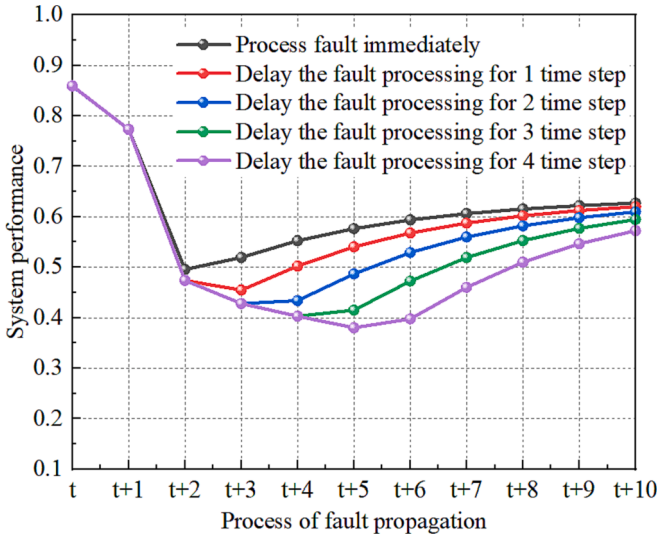

Fig. 13. System performance changes over time in different conditions.

maintenance efficiency and ii) reducing the failure rate. These two aspects can be achieved by increasing the inspection frequency and timely repair, such as the establishing of relevant inspection and repair policies by the plant supervisor and training employees to improve their capability of emergency response (i.e., enhance the effectiveness of safety constraints in Table 2). In particular, safety awareness training should be provided to operators and supervisor to enhance their safety awareness. In this way, the faults may be handled rather than ignored. Besides, safety knowledge training for operators and maintenance workers can effectively reduce the risk of operation and maintenance processes. Furthermore, managers and supervisors should be trained in safety management theory and method training to help them make correct decisions.

5. Discussion

5.1. Comparison with Bayesian network (BN) and DBN for risk assessment

BN is a probabilistic inference technique for reasoning under uncertainty. It can consider conditional dependence and common failures in the accident modeling process, thereby relaxing the limitations of traditional methods (Yuan et al., 2015; Sun et al., 2020). However, BN is a type of directed acyclic network. The interaction and interdependence of components in a complex system make the system a closed-loop network, which BN cannot model. Therefore, STAMP can solve this problem because it views safety as a control problem. It can systematically model the system, which can well express and indicate the complex interdependence between components.

DBN explicitly models the time evolution of a set of random variables on the discrete-time axis. In other words, DBN can process time-series data by combining BN and transition probability (e.g., failure rate and repair rate). DBN can be used to solve closed-loop problem. However, DBN focuses on solving the overall risk of a system and cannot represent risk accumulation at a discrete time. DBN aims to estimate the overall risk of the system at each time slice. The proposed method concentrates on the process of risk accumulation in discrete time slice, which is rarely researched in the existing literature. In other words, the proposed approach can model the process of risk accumulation caused by the state change of each system component. By quantifying the state of each component at each time step, it can help practitioners identify the state of the system and determine when the system or unit must be stopped to repair rather than trying to solve the problem online. With the integration of STAMP and CFPM, the present study provides the opportunity

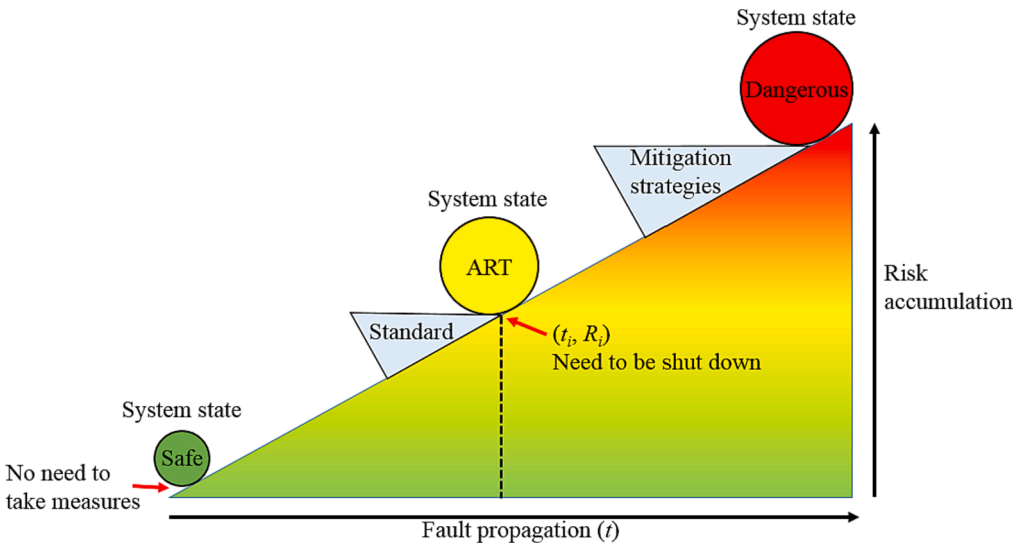

Fig. 14. Schematic diagram of determination of shutdown time.

to generate the risk profile as a probabilistic and time-dependent evolution in a systematic way.

5.2. Determination of shutdown time

The proposed method can help managers and operators determine when repair measures or the shutdown of a system should be under taken to terminate or mitigate the process of risk accumulation to ensure system safety. For example, according to the standards set by the company, the acceptable risk threshold (ART) is R_i.

(1) In the case of ignoring a fault, if the fault in the system has not disappeared before the risk accumulates to R_i at time t_i, repair measures or shutdown must be taken to mitigate or stop the propagation of the fault, which can avoid the accident. However, due to the negligence of operators and managers, those measures will not be taken so that the system risk accumulates over time, which may lead to an accident in the end. The specific information can be seen in Fig. 14.
(2) In the case of dealing with a fault online, to maintain continuous production, operators and managers prefer to deal with a fault online rather than using the Stop Work Authority (CSB, 2014). However, during the maintenance period, the fault still propagates to downstream nodes with a low probability, increasing system risk. In this situation, the proposed method can provide a real-time risk profile and help operators determine when to shut down the system to stop the process of risk accumulation if the fault is not handled efficiently online.

6. Conclusions

Interactions and interdependencies among components become substantial in digitalized process systems. The present study integrates STAMP and CFPM for dynamic quantitative risk assessment of complex systems. The main contribution of the proposed methodology is modeling the system based on system theory and quantify the process of risk accumulation. The proposed approach can help operators to identify the safety constraints and unsafe control actions of a system with the employment of STAMP. Two different CFPMs are proposed by considering the process of fault propagation to assess the dynamic risk of a complex process system. This model can generate a real-time system performance profile, which can be used to help engineers and supervisors to make corrective actions. Besides, it also facilitates the determination of when to take safety measures according to operational procedures and provide an early warning for accidents.

CRediT authorship contribution statement

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

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.

Acknowledgments

The authors gratefully acknowledge the financial support provided by the National Key R&D Program of China (No: 2019YFB2006305) and Central Universities Fundamental Research Funds Project (YCX2021077).

References

Abdulkhaleq, A., Wagner, S., Leveson, N., 2015. A comprehensive safety engineering approach for software-intensive systems based on STPA. Proc. Eng. 128, 2–11.
Adedigba, S.A., Khan, K., Yang, M., 2018. An integrated approach for dynamic economic risk assessment of process systems. Process Saf. Environ. Prot. 116, 312–323.
Altabbakh, H., AlKazimi, M.A., Murray, S., et al., 2014. STAMP – holistic system safety approach or just another risk model? J. Loss Prev. Process Ind. 32, 109–119.
Cai, B.P., Xie, M., Liu, Y.H., Liu, Y.L., Feng, Q., 2018. Availability-based engineering resilience metric and its corresponding evaluation methodology. Reliab. Eng. Syst. Saf. 172, 216–224.
Castilho, D.S., Urbina, L.M.S., Andrade, D., 2018. STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs. Saf. Sci. 108, 129–139.
CBS, 2007. BP America Refinery Explosion Texas City, TX, March 23, 2005, Final Report finding, http://www.csb.gov/, (last checked 16.10.14).
COMAH Competent Authority, Buncefield: why did it happen? HSE Books, 2011. Retrieved on 18 January 2012 from <http://www.hse.gov.uk/comah/ buncefield/buncefield-report.pdf>.
CSB, 2014. Chevron Richmond Refinery Pipe Rupture and Fire California, CA, August 6, 2012 Final Report Finding, http://www.csb.gov/, (last checked 17.11.14).
Department of Emergency Management of Hebei Province Investigation Report on "11·28" Major Deflagration Accident of Hebei Shenghua Chemical Company 2019 http://yjgl.hebei.gov.cn/.

Ding, L., Ji, J., Khan, F., 2020. Combining uncertainty reasoning and deterministic modeling for risk analysis of fire-induced domino effects. Saf. Sci. 129, 104802.
Duan, S.S., Lee, S., Chinthavali, S., Shankar, M., 2018. Best effort broadcast under cascading failures in interdependent critical infrastructure networks. Pervasive Mob. Comput. 43, 114–130.
G. Fu X. Xie Q. Jia Z. Li P. Chen 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. 134 2020 47 82.
Goncalves Filho, A.P., Jun, G.T., Waterson, P., 2019. Four studies, two methods, one accident – An examination of the reliability and validity of Accimap and STAMP for accident analysis. Saf. Sci. 133, 310–317.
Guo, X.X., Ji, J., Faisal, K., Ding, L., Tong, Q., 2021. A novel fuzzy dynamic Bayesian network for dynamic risk assessment and uncertainty propagation quantification in uncertainty environment. Saf. Sci. 42, 237–270. https://doi.org/10.1016/j.ssci.2021.105285.
Hay, A.M., 1977. Tetrachlorodibenzo-para-dioxin release at Seveso. Disasters 4, 289–308.
He, R., Li, X.H., Chen, G.M., Wang, Y.C., Jiang, S.Y., Zhi, C.X., 2018. A quantitative risk analysis model considering uncertain information. Process Saf. Environ. Prot. 118, 361–370.
Hu, J.Q., Zhang, L.B., Ma, L., Liang, W., 2010. An integrated method for safety pre-warning of complex system. Saf. Sci. 48, 580–597.
Jing, K., Du, X.R., Shen, L.X., Tang, L., 2019. Robustness of complex networks: Cascading failuremechanism by considering the characteristics of time delay and recovery strategy. Physica A 534, 122061.
Khakzad, N., 2015. Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. Reliab. Eng. Syst. Saf. 134, 157–168.
Khakzad, N., Landucci, G., Reniers, G., 2015. Application of dynamic Bayesian network to performance assessment of fire protection systems during domino effects. Reliab. Eng. Syst. Saf. 134, 157–168.
Khan, F., Amyotte, P., Adedigba, S., 2021. Process safety concerns in process system digitalization. Educ. Chem. Eng. 34, 33–46.
Khan, B., Khan, F., Veitch, B., 2020. A Dynamic Bayesian Network model for ship-ice collision risk in the Arctic waters. Saf. Sci. 130, 104858.
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.
Li, P., Cheng, Y., Tao, F., 2020. Failures detection and cascading analysis of manufacturing services collaboration toward industrial internet platforms. J. Manuf. Syst. 57, 169–181.
Mannan, M.S., 2005. Lees' loss prevention in the process industries, 3rd ed. Elsevier, Amsterdam.
Mannan, M.S., West, H.H., Krishna, K., Aldeeb, A.A., Keren, N., et al., 2005. The legacy of Bhopal: the impact over the last 20 years and future direction. J. Loss Prev. Process Ind. 18, 218–224.
Mannan, M.S., Chowdhury, A.Y., Reyes-Valdes, O.J., 2012. A portrait of process safety: from its start to present day. Hydrocarb. Process. 91, 55–62.
Ouyang, M., Liu, H., Yu, M., Fei, Q., 2010. STAMP-based analysis on the railway accident and accident spreading: Taking the China-Jiaoji railway accident for example. Saf. Sci. 48, 544–555.
Paltrinieri, N., Oien, K., Cozzani, V., 2012. Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. Reliab. Eng. Syst. Saf. 108, 21–31.
Pasman, H., Sun, H., Yang, M., Khan, F., 2022. Opportunities and threats to process safety in digitalized process systems—an overview. Methods in Chemical Process Safety. Elsevier, Amsterdam, pp. 1–23.
Stanton, N.A., Harvey, C., Allison, C.K., 2019. Systems theoretic accident model and process (STAMP) applied to a Royal Navy Hawk jet missile simulation exercise. Saf. Sci. 113, 461–471.
Sultana, S., Anderson, B., Haugen, S., 2019. Identifying safety indicators for safety performance measurement using a system engineering approach. Process Saf. Environ. Prot. 128, 107–120.
Sun, H., Wang, H., Yang, M., Reniers, G., 2020. 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. 68, 104322.
Sun, H., Wang, H., Yang, M., Reniers, G., 2021. Towards limiting potential domino effects from single flammable substance release in chemical complexes by risk-based shut down of critical nearby process units. Process Saf. Environ. Prot. 148, 1292–1303.
Tong, Q., Yang, M., Zinetullina, A., 2020. A dynamic bayesian network-based approach to resilience assessment of engineering systems. J. Loss Prev. Process Ind. 65, 104152.
Varadharajan, S., Bajpai, S., 2023. Chronicles of security risk assessment in process industries: Past, present and future perspectives. J. Loss Prev. Process Ind. 84, 105096.
Woolley, M., Goode, N., Salmon, P., Read, G., 2020. Who is responsible for construction safety in Australia? A STAMP Analysis. Saf. Sci. 132, 104984.
Wu, Y.P., Chen, Z.L., Zhao, X.D., Gong, H.D., Su, X.C., Chen, Y.C., 2021. Propagation model of cascading failure based on discrete dynamical system. Reliab. Eng. Syst. Saf. 209.
Yang, S.H., Chen, W.R., Zhang, X.X., Yang, W.Q., 2021. A Graph-based Method for Vulnerability Analysis of Renewable Energy integrated Power Systems to Cascading Failures. Reliab. Eng. Syst. Saf. 207, 107354.
Yousefi, A., Hernandez, M., 2020. A novel methodology to measure safety level of a process plant using a system theory based method (STAMP). Process Saf. Environ. Prot. 136, 296–309.
Yuan, Z., Khakzad, N., Khan, F., Amyotte, P., 2015. Risk analysis of dust explosion scenarios using Bayesian networks. Risk Anal. 35 (2), 278–291.
Zhang, Q., Liu, L., Liu, Z., 2021. Application of safety and reliability analysis in wastewater reclamation system. Process Saf. Environ. Prot. 146, 338–349.
Zhang, L.B., Wu, S.N., Zheng, W.P., Fan, J.C., 2018. A dynamic and quantitative risk assessment method with uncertainties for offshore managed pressure drilling phases. Saf. Sci. 104, 39–54.
Zhao, D., Wang, Z.R., Song, Z.Y., Guo, P.K., Cao, X.Y., 2020. Assessment of domino effects in the coal gasification process using Fuzzy Analytic Hierarchy Process and Bayesian Network. Saf. Sci. 130, 104888.
Zhou, X.Y., Liu, Z.J., Wang, F.W., Wu, Z.L., 2021. A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Eng. 222, 108569.
Zhu, R.C., Hu, X.F., Bai, Y.P., Li, X., 2021. Risk analysis of terrorist attacks on LNG storage tanks at ports. Saf. Sci. 137, 105192.
Zinetullia, A., Yang, M., Khakzad, N., Golman, B., Li, X.H., 2021. Quantitative resilience assessment of chemical process systems using functional resonance analysis method and dynamic Bayesian network. Reliab. Eng. Syst. Saf. 205, 107232.