Dynamic Risk Assessment of Chemical Process Systems using System-Theoretic Accident Model and Process (STAMP) and Failure Propagation Model

Sun, Hao; Wang, Haiqing; Yang, Ming; Reniers, Genserik

DOI
10.3303/CET2290051

Publication date
2022

Document Version
Final published version

Published in
Chemical Engineering Transactions

CHEMICAL ENGINEERING TRANSACTIONS
VOL. 90, 2022
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at www.cetjournal.it
Guest Editors: Aleš Bernatík, Bruno Fabiano

ISBN 978-88-95608-88-4; **ISSN** 2283-9216
DOI: 10.3303/CET2290051

Dynamic Risk Assessment of Chemical Process Systems using System-Theoretic Accident Model and Process (STAMP) and Failure Propagation Model

Hao Sun[ab], Haiqing Wang[a]*, Ming Yang[b]*, Genserik Reniers[bcd]

[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
wanghaiqing@upc.edu.cn; m.yang-1@tudelft.nl

Chemical process systems involve complex dynamic processes, and the state of the system often fluctuates during the production process. To ensure the continuation of production, these fluctuations are often ignored or processed online instead of shutting down the unit. However, the interdependence between components in the system is strong, and small fluctuations or faults will be propagated to downstream nodes in turn if the fluctuation is omitted or processed online. A large number of accident investigations prove that the system risk increments as the failure propagates. This may eventually cause the entire system to collapse, causing severe casualties, property losses, and environmental damage. However, little attention has been paid to this type of risk. To measure the dynamic risk profile considering the fluctuation of the production process, this paper proposes a new risk assessment model that integrates the system-theoretic accident model and process (STAMP) and the failure propagation model. Firstly, the STAMP is used to model and analyze the system safety of a process system. An approach is then developed to quantify the risk accumulation of the model based on the failure propagation model. The process of the Chevron Richmond refinery crude unit and its associated upstream process is used to demonstrate the application of the proposed approach.

1. Introduction

Complex systems are developed rapidly, increasing complex interactions and interdependencies among subsystems and components (e.g., technical-human-organizational factors) (Sun et al., 2021). This type of change may pose new threats in process industries. For instance, once a fault occurs in one component, due to the strong interdependence and interactions among components, the fault will be spread to the downstream nodes, causing risk accumulation and the failure of the entire system (Wu et al., 2021). Moreover, some faults are omitted by operators intentionally or unintentionally since they believe that those faults will not impact the system state. Therefore, addressing daily faults timely play a critical role in ensuring system safety. Take the Chevron refinery accident as an example. The loss of containment is found by workers. However, they decided to handle the leakage online to ensure the continuity of production and avoid production losses rather than shutting down the system to ensure system safety. Eventually, this wrong decision brought about a fire accident as the risk accumulated (CSB, 2014). Fortunately, there were no casualties in this accident.
Peer researchers made great contributions and progress on dynamic risk assessment for process industries (Khan et al., 2021). Tong and co-workers (2020) developed a new resilience metric on the basis of dynamic Bayesian network (DBN) to enhance system safety. He et al. (2018) proposed a method based on DBN to assess the system risk in the context of uncertainty. Cai and co-workers (2021) utilized the Markov model and DBN to assess the system risk and measure the system resilience under multiple disasters to ensure system safety. Sun et al. (2021) introduced a novel performance indicator to assess the performance of safety barrier system of process systems. However, few studies have paid attention to how to systematically model the

Paper Received: 12 February 2022; Revised: 2 March 2022; Accepted: 14 May 2022
Please cite this article as: Sun H., Wang H., Yang M., Reniers G., 2022, Dynamic risk assessment of chemical process systems using System-Theoretic Accident Model and Process (STAMP) and failure propagation model, Chemical Engineering Transactions, 90, 301-306 DOI:10.3303/CET2290051

complex system and quantify and measure the dynamic process of the risk accumulation process. DBN is an efficient method to model and assess the system. However, due to the interdependence among components, the information feedback from downstream nodes is instrumental in ensuring system safety, leading to a closed-loop system. DBN is a directed acyclic model and cannot address closed-loop problems. Besides, there is no detailed analysis on quantifying the risk accumulation process when the fault is ignored.
Modelling a system systematically plays key role in the accurate risk assessment. In other words, if the system cannot be accurately modeled, the risk assessment result cannot represent the actual risk of the system. System-theoretic accident model and process (STAMP), as a bottom-up model, is an efficient method for modelling systems systematically (Leveson, 2004). Safety is regarded as a control problem in STAMP. Besides, the STAMP model can be used to analyze the complex interactions between technical-human-organizational factors. Moreover, it can take the feedback from upstream control actions into account (Goncalves Filho et al., 2019). In the light of this (i.e., the accurate system modelling), a novel failure propagation model is developed to show and quantify the process of risk accumulation.
The present study aims to develop a hybrid method, which combines the STAMP model with a new proposed failure propagation model, to measure the risk accumulation process and quantify the dynamic risk assessment to ensure system safety and help operators and managers to make decisions. According to the analysis results of the risk accumulation process, practitioners can determine when the system needs to be shut down to ensure system safety and reduce production losses.

2. The proposed methodology

The methodology is proposed to measure the process risk accumulation and the system risk, which includes two main parts, modeling the system systematically using the STAMP model and quantifying the risk accumulation process in accordance with the proposed cascading failure model.

2.1 STAMP modeling

STAMP regards safety as a control problem. System safety can be ensured if safety constraints are reasonable and efficient. Otherwise, the faults (i.e., the wrong control actions, undesired interactions between components, and external disturbance, etc.) may make the fault propagate to downstream nodes and eventually cause accidents (Sultana et al., 2019). The STAMP method comprises three critical concepts, as shown below.
(1) Safety constraints play an essential role in keeping the system state under a safe range. If the safety constraints, similar to safety barriers, are not taken, or the safety constraints are inefficient, it may result in accidents (Yousefi and Hernandez, 2020).
(2) Control loops are the basis for the system to maintain a safe equilibrium. The commands and information feedback are essential to ensure system safety. Five critical elements consist of control loops: controller, process model, actuator, controlled process, and sensor, respectively.
(3) In the STAMP model, a complex system is viewed as multiple hierarchical structures. In hierarchical structures, the safety constraints and control actions (i.e., commands) are employed by upper-level components to control lower-level components (Leveson, 2004).

2.2 Quantification of the risk accumulation process

STAMP is an effective method to model the system. Nevertheless, it can only analyse the system safety qualitatively. Thus, a quantitative approach (i.e., a novel failure propagation model) is developed in this section to quantify the dynamic risk accumulation process to help operators to identify when the unit or system should be shut down to prevent accidents.

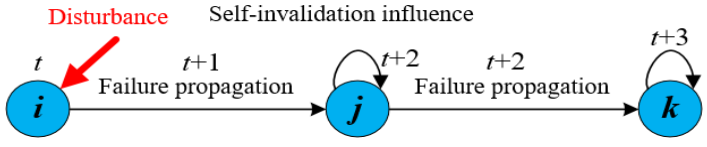

Figure 1: The process of risk accumulation when the fault is ignored

The system state will be changed when the fault occurs. As aforementioned above, to maintain the continuity of production, faults are intentionally ignored by operators and managers. They believe that those faults may not impact the system state. Besides, due to human errors, faults may be ignored unintentionally. In the context of those two situations, the faults will be ignored and propagated to downstream nods, which causes the accumulation of the system risk over time and eventually results in accidents. To quantify the risk

accumulation process, a quantitative approach is presented based on a failure propagation model. The failure probability of component *i* ranges from 0 to 1, and 0 illustrates the node is safe and 1 stands for the node is malfunctioning. The specific process of the risk accumulation based on the proposed failure propagation model is shown in Figure 1. It can be seen from Figure 1, due to the disturbance, node *i* malfunctions at time *t*, and at the next time step (i.e., *t*+1), the fault will propagate to node *j* and affect its state. After this, the fault will be propagated to node *k* at *t*+2. Meanwhile, since node *j* is affected by its previous state, the state of node j starts to decrease at t+2. The rest propagation process can be completed in the same mechanism.

Due to the disturbance that occurs at node *i*, the failure probability of node *i* is defined as 1. The failure propagation probability is dependent on the conditional probability $P(j|i)$. Thus, the failure probability of node *j* at time *t*+1 can be determined by Eq(1).

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

where $P_i(t)$ is the failure probability of node *i* at time *t*, $P(j|i)$ stands for the failure propagation probability, which is assumed as 0.3 in this case.

At time *t*+2, the impact of node *j* affected by itself can be determined by its own failure coefficient *w* multiplied by its failure probability at time *t*+1. Therefore, the failure probability of node *j* at *t*+2 can be calculated by Eq(2).

$$P_j(t+2)=P_i(t+1)\cdot P(j|i)+w_j\cdot P_j(t+1) \tag{2}$$

where w_j indicates the failure coefficient of node *j*, which can be determined by the degree of node *j*, which is defined as Eq(3).

$$w_j=1/(1+d_j) \tag{3}$$

where d_j denotes the number of nodes connected to node *j*. The greater the node degree, the more influential the node is in the system. In practice, the more important the node, the higher the degree of safety in design, and the less it is affected by itself.

It can be concluded that the failure probability of node *j* when it is affected by node *i* and itself at time t_x ($t_x \geq 2$) is:

$$P_j(t_x)=P_i(t_x-1)\cdot P(j|i)+w_j\cdot P_j(t_x-1) \tag{4}$$

If two or more nodes jointly impact the node j, its failure probability can be determined by Eq(5) (adapted from Wu et al., 2021).

$$P_j(t_x)=1-\prod_{u=1}^{n}(1-Pu(t_x-1)\cdot P(j|u))+w_j\cdot P_j(t_x-1) \tag{5}$$

where *u* illustrates a node that affects node *j*, *n* is the number of nodes that affect node *j*. It is worth noting that node *j* can be viewed as a failed node when $P_j(t_x)=1$.

Moreover, another situation exists, when two nodes fail, they will influence the downstream nodes at the same time, similar to the AND gate in the fault tree. For example, if the electric generator fails, the standby one can be employed to maintain the normal function to ensure system safety. However, when the two electric generators fail at the same time, it will affect the normal operation of the system. In this situation, Eq(5) can be converted to Eq(6) (adapted from Wu et al., 2021) to calculate the failure propagation process:

$$P_j(t_x)=\prod_{u=1}^{n}(Pu(t_x-1)\cdot P(j|u))+w_j\cdot P_j(t_x-1) \tag{6}$$

In the light of Eq(4) and Eq(5), the failure probability of all nodes for the system can be quantified. Finally, the system risk can be determined by Eq(7).

$$R_s(t)=\frac{\sum_{a=1}^{m} fa\cdot \mathrm{Pa(t)}}{\sum_{a=1}^{m} fa} \tag{7}$$

where R_s denotes the system risk, *m* is the total number of nodes of the system, *t* is the time, which satisfies $0\leq t\leq t_f$, t_f represents the time when the system fails completely, f_a means the weight of node *a*, which can be calculated by Eq(8).

$$F_a=d_a/m \tag{8}$$

where d_a is the number of nodes connected to node *a*, which means that the more important the node, the greater the impact of its state on the system.

3. Case study

3.1 Descriptions of the case

The fire accident resulted from a pipe rupture in the “Chevron Richmond refinery” occurred on August 6, 2012 (Adedigba et al., 2018). The loss of containment is discovered by operators. To maintain the continuity of production and avoid the production losses caused by the unnecessary shutdown, the managers decided to neglect the fault and deal with the leakages online instead of using the Stop Work Authority (CSB, 2014), which eventually led to the fire accident. The process of the Chevron Richmond refinery crude unit and its associated upstream process are represented in Figure 2, which illustrates the proposed methodology.

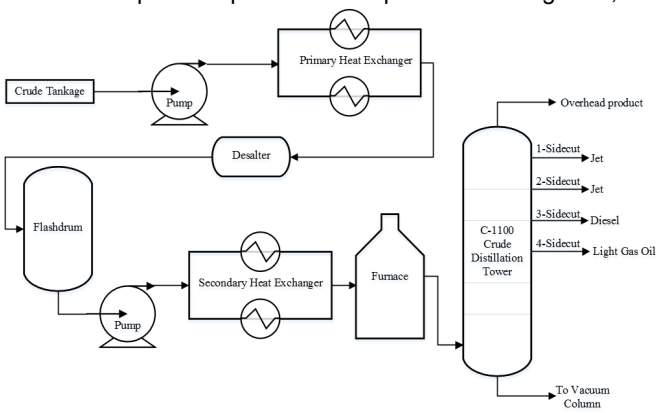

Figure 2: Schematic diagram of the Chevron Richmond refinery crude unit

3.2 STAMP modeling for Richmond refinery crude unit

The abovementioned process is a typical complex system. To accurately quantify the system risk, the primary step is modelling the system in accordance with system theory. In present study, the complex system is modelled by the STAMP model.

The first task of modelling the system is to determine the system boundaries. The abovementioned process is regarded as the system boundary. In accordance with STPA and STAMP methods, the control structure of the system is presented in Figure 3a.

Figure 3a shows the control structure of the system, where the downward arrows are control actions for applying safety constraints to the downstream nodes, and the downward dashed arrows present control actions from site operators using safety constraints to the downstream nodes. Moreover, the upward dashed arrows stand for feedback, which provides information on how the parameters in the system change over time and how effectively the control actions are performed. Because of the effect among the components for the system, the upstream components states will impact the downstream components states. Thus, the network diagram (i.e., Figure 3b) can be extracted from Figure 3a.

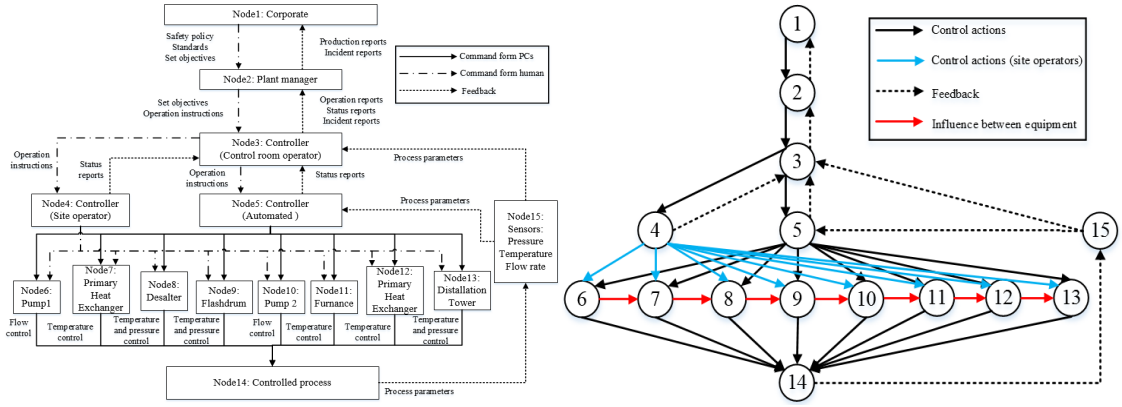

Figure 3: a) Control structure and b) corresponding network diagram of the Richmond refinery crude unit system

3.3 Quantification of the risk accumulation process

Due to human errors, the fault is neglected, resulting in the state change of downstream nodes. In other words, there is no maintenance intervention to cut off or mitigate the propagation since the fault is omitted or the fault is considered to have no impact on the system, leading to the decrease in the system state and increase in the system risk over time. In order to quantify and show the process of risk accumulation, assume that the fault occurs on node 3. Owing to the complex interdependences and interactions among nodes, many nodes may jointly impact one node. Take node 3 as an example, in Figure 3b, node 3 is influenced by node 2, node 4, node 5, and node 15, which indicates that the feedback from downstream nodes is critical information to help to maintain the system under a safe range. This demonstrates that the developed method not only takes the interaction between components into account but also includes the impact of information feedback from downstream nodes. Furthermore, this shows that the presented approach can accurately model complex systems, which quantifies the actual risk accumulation process.

In accordance with the developed failure propagation model, the node state can be measured by Eq(4), Eq(5), and Eq(6). According to Eq(7), the dynamic processes of risk accumulation (i.e., the system risk) change over time can be seen in Figure 4. In Figure 4, due to the fault being neglected, there are no maintenance activities involved, resulting in the fault propagating to downstream nodes, and the system risk increases gradually over time. Note that when the fault of the node spreads to the downstream node, the information feedback of the downstream node may influence the node, leading to an increase in the node failure probability. This is a vicious circle, exacerbating the process of risk accumulation. For instance, assume that node 3 is affected by a disruption (i.e., a fault) at time *t*, the fault will be spread to node 4 and node 5 at *t*+1. At *t*+2, the fault will be propagated from nodes 4 and 5 to downstream nodes (i.e., node 6, 7, 8, etc.). Meanwhile, nodes 4 and 5 will be affected by themselves at the same time. Moreover, the information feedback from node 4 and node 5 may influence the state of node 3 at time *t*+2. Furthermore, the information from node 15 will decrease the state of node 5 at time *t*+5. In the light of this type of fault propagation, the system risk may reach a high value rapidly.

The engineering meaning of the proposed approach is to provide the process of risk accumulation caused by fault propagation in the system. The traditional methods of dynamic risk assessment are to assess the risk of the entire system in different time slices without detailing the state changes of each node over time. Compared with the traditional risk assessment method, the developed approach quantifies the risk accumulation process and system risk in minute details, which can be used to help operators and managers to determine when they should take necessary maintenance measures or shut down the system to prevent accidents instead of maintaining the production continuity to avoid production losses. For example, according to the acceptable risk threshold (ART) formulated by managers (e.g., ART=0.3), it can be seen from Figure 4 that the maintenance activities must be taken to mitigate the propagation of the fault before t+3 or the system must be shut down before t+3 to stop the fault propagation to reduce the system risk.

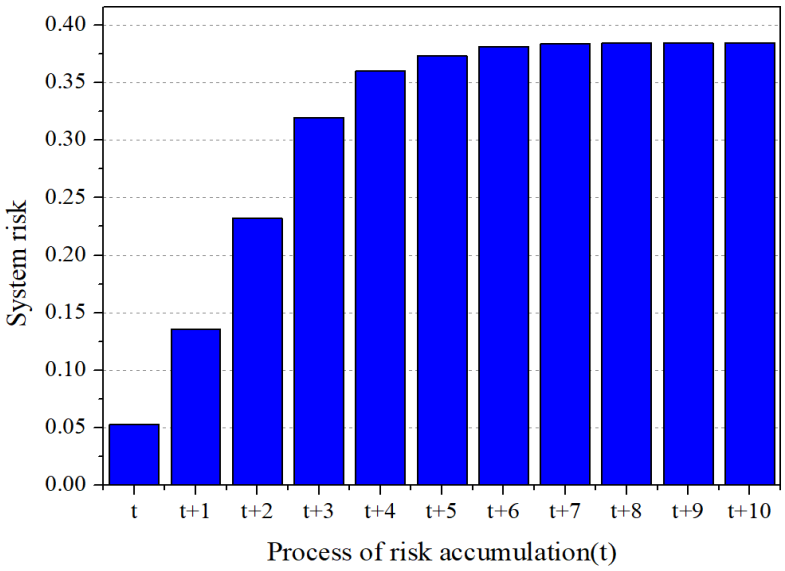

Figure 4: Process of risk accumulation when a fault is ignored

4. Conclusions

Process systems are typical complex systems involving complicated interactions and interdependencies between subsystems and elements. Once a fault occurs at one node, it will propagate to downstream nodes, and the error information feedback may influence the state of upstream nodes, which will increase the system risk rapidly. The present study combines STAMP with failure propagation model to systematically model the complex system and quantify the system risk over time. The main contribution of the presented methodology is modelling the system on the basis of system theory and providing a detailed risk accumulation process for practitioners to determine when actions (e.g., maintenance activities, emergency shutdown, etc.) need to be taken. Besides, the proposed approach can help operators to identify the safety constraints and unsafe control actions of a system with the employment of STAMP. A novel failure propagation model is proposed to quantify the process of risk accumulation, which can generate a real-time risk profile and help operators to determine when to take safety measures and provide an early warning for accidents.

Acknowledgments

The authors gratefully acknowledge the financial support provided by the Central Universities Fundamental Research Funds Project (YCX2021077).

References

Adedigba, S.A., Khan, F., Yang, M., 2018. An integrated approach for dynamic economic risk assessment of process systems. Process. Saf. Environ. Prot. 116, 312–323.

Cai, B.P., Zhang, Y.P., Wang, H.F., Liu, Y.H., Ji, .R.J., Gao, C.T., Kong, X.D., Liu, J., 2021. Resilience evaluation methodology of engineering systems with dynamic-Bayesian-network-based degradation and maintenance. Reliab. Eng. Syst. Saf. 209, 107464.

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).

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.

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.

Jafari, M.J., Pouyakian, M., Khanteymoori, A., Hanifi, S.M., 2020. Reliability evaluation of fire alarm systems using dynamic Bayesian networks and fuzzy fault tree analysis. J. Loss Prev. Process. Ind. 67, 104229.

Khan, F., Amyotte, P., Adedigba, S., 2021. Process safety concerns in process system digitalization. Education for Chemical Engineers, 34, 33-46.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.

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., 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.

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, 107424.

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.