Dynamic-risk-informed safety barrier management

An application to cost-effective barrier optimization based on data from multiple sources

Yuan, Shuaiqi; Reniers, Genserik; Yang, Ming

DOI
10.1016/j.jlp.2023.105034

Publication date
2023

Document Version
Final published version

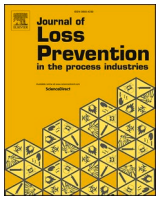
Published in
Journal of Loss Prevention in the Process Industries

Journal of Loss Prevention in the Process Industries 83 (2023) 105034

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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



Dynamic-risk-informed safety barrier management: An application to cost-effective barrier optimization based on data from multiple sources

Shuaiqi Yuan [a,*], Genserik Reniers [a,b,c,**], Ming Yang [a,d,e]

[a] Safety and Security Science Section, Faculty of Technology, Policy and Management, TU Delft, Delft, the Netherlands
[b] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000, Antwerp, Belgium
[c] CEDON, KULeuven, 1000, Brussels, Belgium
[d] Centre of Hydrogen Energy, Institute of Future Energy, Universiti Teknologi Malaysia, 81310, UTM Johor Bahru, Johor, Malaysia
[e] National Centre of Maritime Engineering and Hydrodynamics, Australia Maritime College, University of Tasmania, Launceston, Tasmania, Australia

ARTICLE INFO

Keywords:
Safety barrier management
Dynamic risk assessment
Cost-effectiveness analysis
Bayesian updating
Safety barrier degradation
Condition monitoring

ABSTRACT

An integrated approach for performance assessment and management of safety barriers in a systemic manner is needed concerning the prevention and mitigation of major accidents in chemical process industries. Particularly, the effects of safety barriers on system risk reduction should be assessed in a dynamic manner to support the decision-making on safety barrier establishments and improvements. A simulation approach, named Simulink-based Safety Barrier Modeling (SSBM), is proposed in this paper to conduct dynamic risk assessment of chemical facilities with the consideration of the degradation of safety barriers. The main functional features of the SSBM include i) the basic model structures of SSBM can be determined based on bow-tie diagrams, ii) multiple data (periodic proof test data, continuous condition-monitoring data, and accident precursor data) may be combined to update barrier failure probabilities and initiating event probabilities, iii) SSBM is able to handle uncertainty propagation in probabilistic risk assessment by using Monte Carlo simulations, and iv) cost-effectiveness analysis (CEA) and optimization algorithms are integrated to support the decision-making on safety barrier establishments and improvements. An illustrative case study is demonstrated to show the procedures of applying the SSBM on dynamic risk-informed safety barrier management and validate the feasibility of implementing the SSBM for cost-effective safety barrier optimization.

1. Introduction

The application of the barrier concept in the safety science domain has a long history. Various models use the barrier concept or similar concepts to demonstrate the protection of technical or non-technical measures on target objects from hazards, such as the energy model (Gibson, 1961), bow-tie (CCPS/EI, 2018), LOPA (CCPS, 2001), and the Swiss cheese model (Reason et al., 2006). However, conceptual accident analysis models cannot evaluate the intervention of safety barriers in a quantitative manner, and thus can only provide limited information and supports for safety barrier management. By contrast, the integration of quantitative risk assessment (QRA) and the safety barrier concept naturally has the advantage of assessing the intervention of the safety barriers quantitatively in the form of risk-associated indicators. For instance, the European ARAMIS (Accidental Risk Assessment Methodology for Industries) project integrated QRA and safety barrier assessment to facilitate the audit and management of safety barriers (Andersen et al., 2004). In the last decades, the development of approaches for safety barrier performance assessment and management has attracted more and more attention. Landucci et al. (2015) proposed a LOPA (layer of protection analysis) based method for quantitative assessment of safety barrier performance in preventing the escalation of fire-induced domino effects. Then, this methodology was adapted to the performance assessment of safety barriers in Natech event scenarios by characterizing the effectiveness and PFD (probability of failure on demand) of safety barriers (Misuri et al., 2020, 2021). Bayesian network (BN) was also used to support safety barrier assessment under different accident scenarios. Khakzad et al. (2017) applied a dynamic Bayesian network (DBN) for the performance assessment of fire protection systems with respect to domino effect scenarios. Zeng et al. (2020)

* Corresponding author. S.Yuan-2@tudelft.nl.
** Corresponding author. G.L.L.M.E.Reniers@tudelft.nl.
E-mail address: S.Yuan-2@tudelft.nl (S. Yuan).

https://doi.org/10.1016/j.jlp.2023.105034
Received 30 December 2022; Accepted 13 March 2023
Available online 15 March 2023

employed DBN to model the spatial-temporal propagation of domino effects and to estimate the dynamic probabilities of domino chains considering the impact of add-on safety barriers. DIMAIO et al. (2021) proposed an approach for the performance assessment of safety barriers based on multistate BN accounting for safety barriers degradation in the risk assessment of oil and gas systems. A hybrid DBN embedding multiphase Markov (MSMM) process was developed for dynamic performance prediction of safety barriers and supporting the decision-making on barrier maintenance (Wu et al., 2022). Additionally, the analytical formulas and modeling approaches for performance evaluation of digitalized safety barriers were introduced by (Zhang and Liu, 2022). Yuan et al. (2022b) proposed an approach for the performance assessment of safety barriers under toxic gas leakage scenarios by integrating computational fluid dynamics (CFD) and evacuation modeling.

In terms of safety barrier management, Johansen and Rausand (2015) discussed the main principles related to barrier management in the offshore oil and gas industry and emphasized the need for integrating a systematic approach to risk management and safety barrier management. CCPS (USA) and Energy Institute (UK) developed guidance on employing bow-tie diagrams to facilitate safety barrier management through the proper depiction and allocation of safety barriers (CCPS/EI, 2018). Similarly, bow-tie diagrams were employed to support accident process monitoring and barrier alarm management based on the inspection of barrier status (Schmitz et al., 2020, 2021). An approach based on bow-tie was proposed to support the identification of integrated safety and security barriers Yuan et al. (2022c). By integrating safety barrier assessment into a QRA framework, the effectiveness (risk-reduction performance) of barriers can be reflected by how much risk can be reduced by implementing such barriers and further making decisions based on the comparison of risks to achieve risk-based safety barrier management.

Moreover, the dynamic barrier management concept was introduced by Pitblado et al. (2016), in which the usage of multiple data sources for determining near-real-time barrier status was suggested. To develop a dynamic barrier management approach, updating safety barrier status and risk profiles is necessary when new information becomes available over time. Bayes' theorem was introduced to achieve dynamic risk assessment of chemical process systems by using near misses and incident data to update accident likelihood and the failure probability of safety barriers (Kalantarnia et al., 2009, 2010; Khakzad et al., 2012). Additionally, there are some attempts to use condition-monitoring data for dynamic risk assessment (DRA). For instance, condition-monitoring data was employed to estimate the degradation states of chemical process systems with the help of Kalman filtering (Zadakbar et al., 2013a), particle filtering (Zadakbar et al., 2015), and principal component analysis (Zadakbar et al., 2013b). Zeng and Zio (2018) integrated statistical failure data and condition-monitoring data for dynamic risk assessment of a high-flow safety system by using a Bayesian updating algorithm. In PRA (probabilistic risk assessment) and DRA, probability distributions are widely-used to interpret uncertainty (Yazdi et al., 2019). Thus, the handling of uncertainty propagation in DRA/PRA should be properly addressed to facilitate risk-based safety barrier management.

Considering the limited budget faced by chemical companies, the trade-off between accident risk levels and the investment in safety barrier establishment and management is another important issue (Chen and Reniers, 2021). How to make decisions on cost-effective safety barrier management based on dynamic risks is challenging, particularly considering the utilization of data from multiple sources for risk updating. As discussed above, new approaches and tools for dynamic risk-informed safety barrier management need to be developed. We identify several challenges that need to be tackled in terms of dynamic risk-informed safety barrier management.

- i) The integration of dynamic risk assessment with safety barrier management procedures needs to be enhanced. A comprehensive tool should be developed to integrate dynamic risk assessment and cost-efficient decision-making on safety barrier management.
- ii) Interactions and interdependency between safety barriers/barrier components should be considered in the barrier failure assessment. Meanwhile, barrier failure assessment and DRA should be integrated and performed in a unified tool.
- iii) Multiple data (real-time monitoring data, barrier inspection data, accident precursor data, etc.) may be used to update failure probabilities of safety barriers and initiating event probabilities, and thus to update risk profiles and facilitate dynamic safety barrier management.
- iv) Uncertainty propagation in DRA needs to be handled. Meanwhile, decision-making on safety barrier management based on dynamic risks needs to be further investigated from a cost-effective perspective.

To fill the identified gaps, this study proposes a safety barrier modeling tool, named Simulink-based safety barrier modeling (SSBM), for performance assessment and dynamic management of safety barriers based on the MATLAB/Simulink platform (Chaturvedi, 2017). Bow-tie analysis/safety barrier diagram analysis, dynamic risk assessment techniques, Monte Carlo simulation, cost-effectiveness analysis (CEA), and optimization algorithms are integrated into the SSBM with a variety of functionalities to support the dynamic risk-informed safety barrier management. The remainder of this paper is organized as follows. Firstly, the proposed methodology is introduced in section 2. Then, an illustrative case study is employed in section 3 to demonstrate the application of the proposed approach in dynamic risk assessment and cost-effective safety barrier optimization. Followed by the discussions are given in section 4, and conclusions are presented in section 5.

2. Methodology

2.1. Overview of the proposed approach

Simulink is a MATLAB-based graphical programming environment for modeling, simulating, and analyzing multidomain dynamical systems (Chaturvedi, 2017). Due to several advantages of Simulink, such as its user-friendly primary interface, customizable block libraries, and good compatibility with the rest of the MATLAB environment, the Simulink programming environment is a good option for the development of safety barrier modeling with multiple functionalities. Therefore, a dynamic-risk-informed safety barrier management approach is proposed, and the Simulink-based safety barrier modeling (SSBM) is developed for implementing the proposed approach in practice. The flowchart of the proposed approach is illustrated in Fig. 1, and a detailed elaboration on the three main steps of the approach is given in the following sub-sections.

2.2. Transform the bow-tie/safety barrier diagram to a simulink model (step 1)

This step aims to build accident scenarios with the consideration of the intervention of safety barriers. A bow-tie diagram, which is a combination of a fault tree and an event tree, is widely used to conduct HAZard IDentification (HAZID) and demonstrate the linkages between safety barriers and specific hazards. It is suggested to implement the bow-tie technique for HAZID, then followed by constructing safety barrier diagrams (SBDs) by placing safety barriers on the paths of the bow-tie diagrams (Duijm, 2009).

2.2.1. Basic rules for safety barrier modeling

The safety barrier diagram (SBD) was introduced by Duijm (2009) as a safety management tool. It can be regarded as a modified version of the

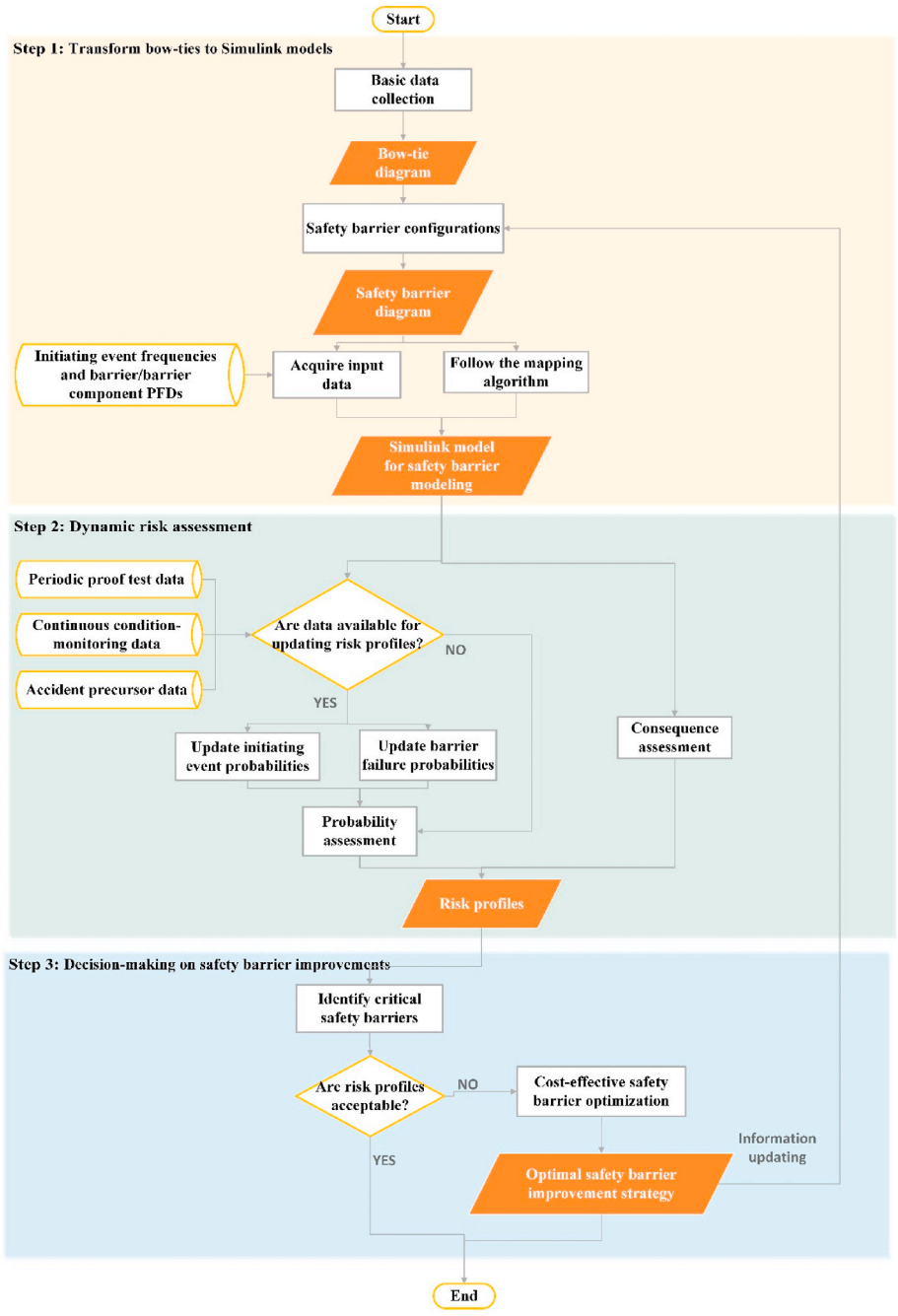


Fig. 1. Flowchart of the dynamic-risk-informed safety barrier management approach.

bow-tie diagram, and it has the advantages of i) relative simplicity that supports communication with non-expert stakeholders, ii) having deliberately inserted safety systems that support the management and maintenance of these systems, and iii) providing a useful framework for integrating information from risk analysis with operational safety management. A comparison between the conventional bow-tie diagram and the SBD is shown in Fig. 2. The main difference between SBD and BT/fault tree exists in the demonstration of safety barriers/add-on safety systems in the diagrams, as shown in Fig. 2. According to the basic requirements of safety barriers suggested by (CCPS/EI, 2018), a safety barrier should be a complete system fulfilling the criteria of being effective, independent, and auditable, which means a safety barrier should be capable of performing the complete intended function on its own when demanded. Among the intermediate events in an event tree, some can be presented as safety barriers because they meet the above-mentioned requirements some cannot. Although in some previous studies, all of those intermediate events were called safety barriers, we do not consider some of them (such as ignition and confined space nearby) as safety barriers. For those intermediate events that cannot be managed and do not meet the requirements of a safety barrier, we call them escalation factors/events.

The calculation rules considering the failure of safety barriers are presented as follows:

$$P_{OUT1} = P_{IN} * PFD \tag{1}$$

$$P_{OUT2} = P_{IN} * (1 - PFD) \tag{2}$$

where P_{IN} is the input probability for the safety barrier. P_{OUT1} is the output probability of the branch with the condition that the safety barrier failed and P_{OUT2} is the output probability of the branch with the

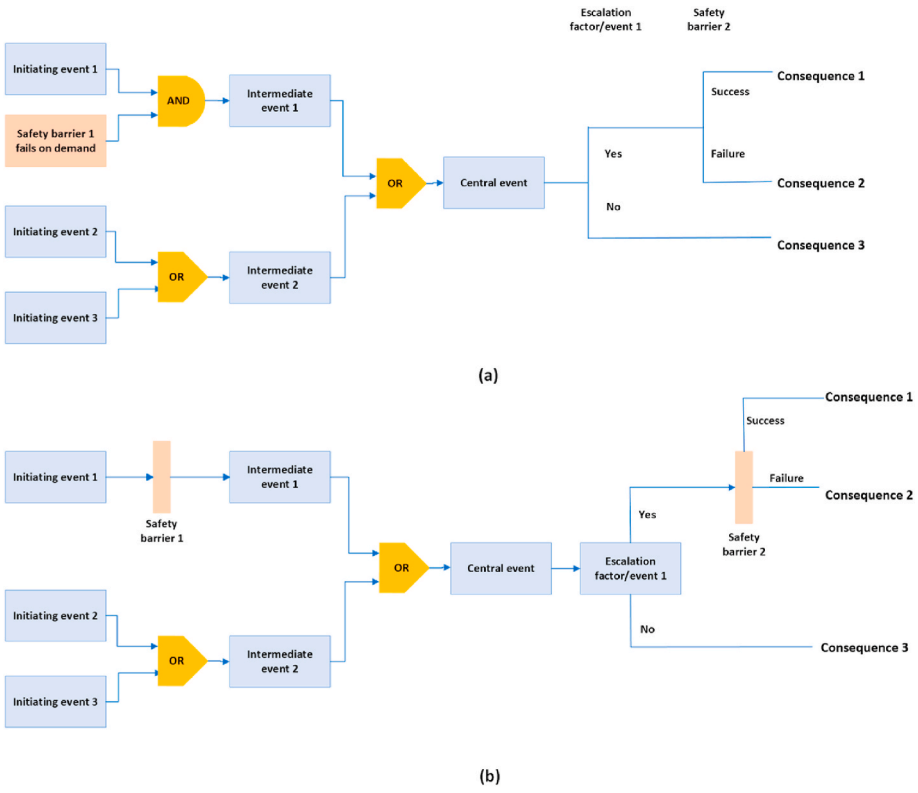


Fig. 2. A comparison between the conventional bow-tie diagram (top) and the safety barrier diagram (bottom).

condition that the safety barrier functioned. *PFD* is the probability of failure on demand of this barrier. On the left-hand of the SBD, multiple barriers may be located before an undesired event on the same branch. In that case, the output probability of this branch can be calculated by formula (3).

$$P_{OUT} = P_{IN} * (PFD_1 * PFD_2 \cdots PFD_n) \tag{3}$$

where P_{OUT} is the output probability and P_{IN} is the input probability of this branch. PFD_1 to PFD_n denote the PFDs of safety barriers, and n is the number of barriers located on this branch. This equation is valid under the assumption that the occurrence of failure of each safety barrier in this branch is independent.

2.2.2. *Mapping algorithm*

Previous studies already investigated the implementation of MATLAB/Simulink simulations for the construction of fault trees (Latif-Shabgahi and Tajarrod, 2009; Papadopoulos and Maruhn, 2001) and the reliability analysis of safety instrumented systems (Ouache et al., 2015). To enhance the flexibility and adaptability of the SSBM, this paper suggests developing all the elements (exclude arrows/linkages) of the bow-tie diagram or SBD as sub-systems in the Simulink simulations.

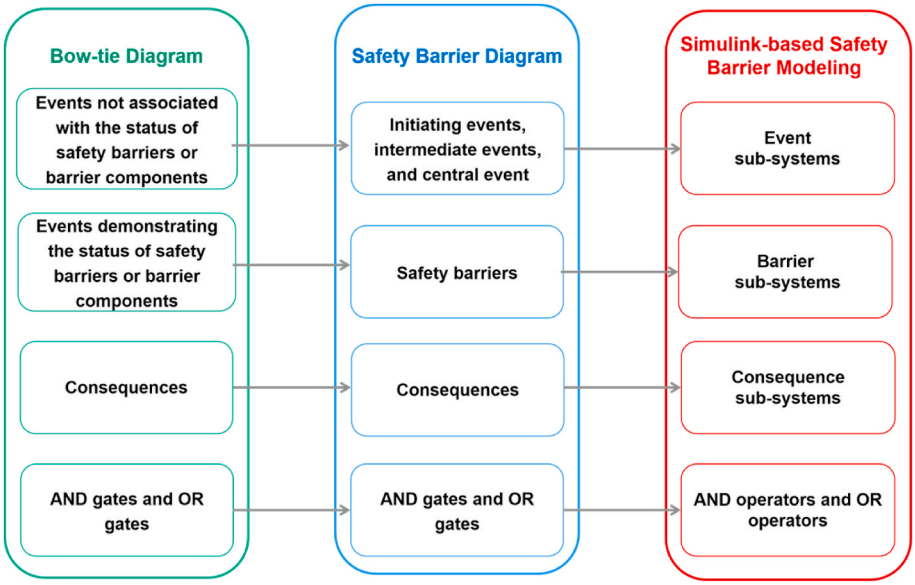


Fig. 3. A mapping algorithm reflecting the relationships between conventional bow-tie diagram, SBD, and SSBM.

Then, the configuration of the elements can be made by developing specific simulation structures inside the sub-systems according to the needs of users. The basic rules for probability calculation are adapted from the fault tree (Haasl et al., 1981) and event tree (Andrews and Dunnett, 2000). The mapping relations between the elements in a conventional bow-tie, SBD, and the sub-systems in SSBM are presented in Fig. 3.

Additionally, a sub-system named "management delivery system" is also added to the SSBM. Management delivery system (MDS) was defined as a set of organizational and management factors that can prevent or mitigate undesired events indirectly and mainly play roles by enhancing/maintaining the performances of the scenario-specific safety barriers or increasing the accident response capabilities of the overall system (Yuan et al., 2022a). As shown in Fig. 4, an example of SSBM is presented corresponding to the bow-tie and SBD in Fig. 2. Table 1 shows the features/tasks of each sub-system in the SSBM.

2.2.3. PFD calculation of safety barriers

The implementation of fault tree analysis (FTA) or reliability block diagram (RBD) helps to determine the PFD of a complex safety barrier system considering the failures of different components of the barrier system. In SSBM, a hierarchical structure for reliability analysis of safety barrier systems can be easily obtained by using hierarchical sub-systems due to the flexibility and adaptability of the Simulink platform. For instance, for a safety barrier system with the elements/functionalities of 'detect-decide-act', the different functionalities should be achieved by using different components. The corresponding structure for this safety barrier system can be represented by a fault tree inside the "barrier sub-system", as shown in Fig. 5. After the PFD of this safety barrier system was determined, the probabilities/frequencies for the outlet branches should be calculated and output according to formulas (1) and (2).

Additionally, several safety barriers may have common components. If those safety barriers with shared components were located on the same branch, the conditional probabilities should be used for the safety barriers excluding the first occurrence barrier (the barrier that may fail first). For example, two safety barriers with a shared component are presented in Fig. 6. In that case, a conditional probability $P_2^{'}$ should be used for barrier 2 given the failure of barrier 1. The conditional probability can be calculated as follows (Duijm, 2009):

$$P_{2,R} = \frac{P_2 - P_C}{1 - P_C} \tag{4}$$

$$P_2^{'} = P(B_2\ fails\ |B_1\ has failed)$$

$$= P_{2,R} + P(C\ fails \mid B_1\ has failed)\left[1 - P_{2,R}\right]$$

Table 1
Features/tasks of each sub-system in the SSBM.

Sub-systems	Features/tasks	Sub-systems	Features/tasks
Event	Event sub-systems contain and transport the frequencies or probabilities (or probability distributions in case of handling uncertainty propagation) of such events happening.	Barrier	Barrier sub-systems aim to determine the PFDs of such safety barriers and calculate and output the probabilities/frequencies for outlet branches. For complex safety barrier systems, the PFDs can be calculated with the help of fault tree analysis or reliability block diagrams.
Consequence	Consequence sub-systems contain and transport information associated with both the frequencies/ probabilities and the severities of such consequences.	MDS	MDS sub-systems collect information, including both the probabilities/ frequencies and severities of the consequences, from the consequence sub-systems and transport necessary parameters to barrier sub-systems for safety barrier configurations and PFD calculation. Decision-making modules can be incorporated into the MDS sub-systems.
AND operator	AND operators receive frequencies/ probabilities from the inlets and calculate and output the frequencies/ probabilities for the outlet by following an "AND" logic.	OR operator	OR operators receive frequencies/probabilities from the inlets and calculate and output the frequencies/probabilities for the outlet by following an "OR" logic.

$$= P_{2,R} + (P_C / P_1)\left[1 - P_{2,R}\right] \tag{5}$$

where P_1 presents the PFD of the whole barrier 1, which contains a common component C with a PFD P_C. P_2 presents the PFD of the whole barrier 2, which also contains the component C. $P_{1,R}$ presents the PFD of the remaining components of the barrier 1 in series with component C. $P_{2,R}$ presents the PFD of the remaining components of the barrier 2 in series with component C. The above formulas can also be extended and adapted to calculate the conditional probabilities of multiple barriers with a shared component and located on the same branch of the SBD.

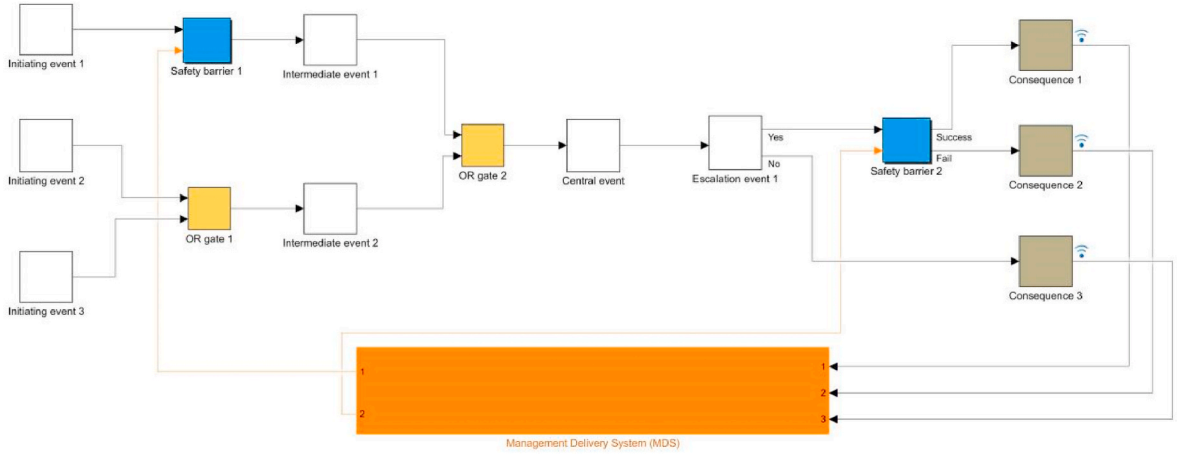


Fig. 4. Barrier modeling based on Simulink simulation.

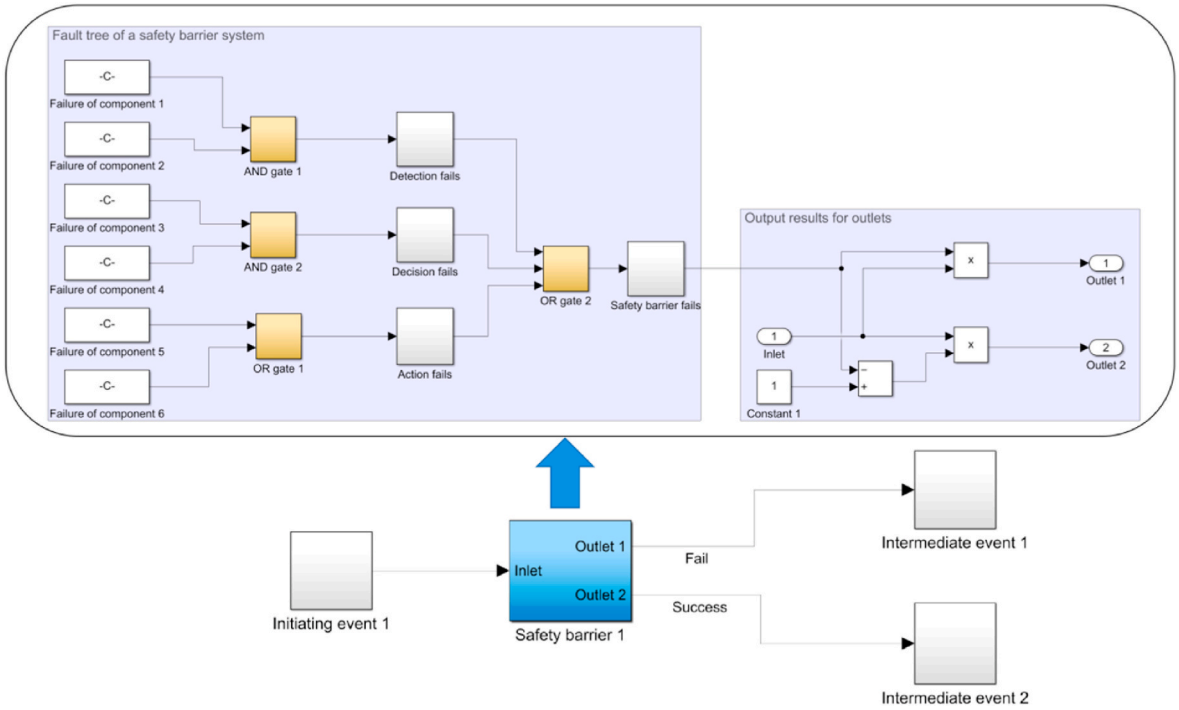


Fig. 5. A safety barrier system illustrated by a barrier sub-system in the SSBM.

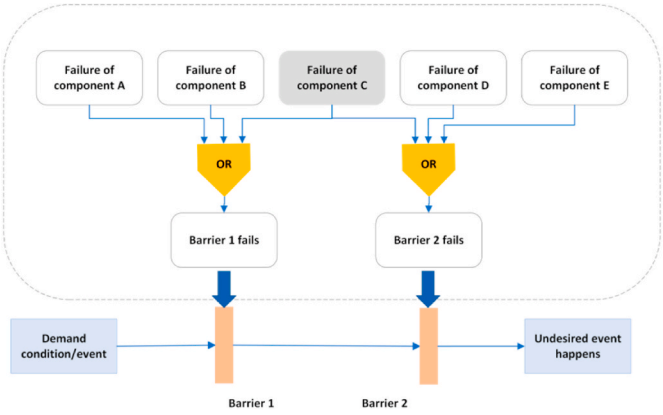


Fig. 6. Two safety barriers with a shared component.

2.3. Dynamic risk assessment (step 2)

Based on the Simulink model developed in step 1, a probabilistic risk assessment (PRA) can be performed after making some configurations to the sub-systems of the model. The inputs of the PRA are the probabilities of the happening of the initiating events and the PFDs of safety barrier components. Additionally, various data are employed to update the failure probabilities of safety barriers and the probabilities of the happening of initiating events to achieve a dynamic risk assessment (DRA). With DRA performed by the SSBM, updated risk profiles may be utilized to support safety barrier optimization by using a decision-making module.

2.3.1. Data sources for updating risks

In previous studies, statistical failure data, for instance, the counts of incidents or near-misses from the same or similar systems, were widely-used for barrier failure probability updating and risk updating based on Bayes's theorem (Meel and Seider, 2006; Kalantarnia et al., 2009; Khakzad et al., 2012). However, there are some unavoidable difficulties in collecting enough statistical failure data and fully reflecting system-specific features of the target system by using accident precursors of similar systems (Zeng and Zio, 2018). Generally, safety barriers follow a low-demand mode. Periodic proof tests are implemented to evaluate the health status of safety barriers, particularly for the final elements of the safety-instrumented systems (SISs), which are posed to degradations caused by harsh working environments (Zhang et al., 2020). Health indicators of barrier status obtained from the periodic proof tests are useful in terms of dynamic failure assessment of safety barriers. Additionally, the collection and analysis of real-time condition-monitoring data of process systems also provide the opportunity to update the failure probability of the target system and further update risk profiles. Some real-time information obtained from condition monitoring (temperature, pressure, vibration, etc.) helps to measure the degradation states of the target systems and obtain more accurate failure rates (Zeng and Zio, 2018). Therefore, periodic proof test data of barrier health status and continuous condition-monitoring data of process systems are also introduced in this study to combine with the accident precursor data to update the risk profiles. Moreover, as an alternative approach to mathematical analytic methods, the implementation of Monte Carlo simulations helps to handle the calculation of probability distributions in PRA (Hickman, 1983; Hauptmanns, 2002; Manno et al., 2012). By implementing Monte Carlo simulations based on the SSBM, the proposed approach is able to perform dynamic risk assessment involving both deterministic probability point values and probability distributions. A detailed elaboration on the risk updating methods is presented in the following sub-sections.

2.3.2. Bayesian updating by using accident precursor data

Probability distributions were introduced and widely used to support the interpretation of uncertainty in fault-tree-based risk assessment approaches (Yazdi et al., 2019). Beta distributions and gamma distributions were used to describe failure probabilities because they have advantages in serving as prior distributions in the Bayesian estimation of parameters (Eide et al., 2007; Khakzad et al., 2012). Beta-binomial model and Gamma-Poisson model were used as the base for conducting Bayesian updating of failure probabilities in PRA (Siu and Kelly,

1998). In this study, the Beta-binomial model is used, and the Beta distributions are suggested to describe prior PFDs of safety barriers or safety barrier components. Beta distribution can be presented as follows:

$$f(\mu)=\frac{\tau(a+b)}{\tau(a)\tau(b)}\mu^{a-1}(1-\mu)^{b-1}\propto\mu^{a-1}(1-\mu)^{b-1},a>0,b>0 \tag{6}$$

where $f(\mu)$ is a Beta distribution of μ. a and b are distribution parameters. $\tau(a)=\int_0^\infty t^{a-1}e^{-t}\,dt$ is a gamma function. Generally, prior probability distributions are derived from the failure database or expert opinions to describe the uncertainty in failure probabilities. When new accident precursor data becomes available, the prior probability distributions can be updated using Bayes's theorem and obtaining posterior probability distributions, as follows:

$$f(x\mid Data)=\frac{g(Data\mid x)f(x)}{\int g(Data\mid x)f(x)dx}\propto g(Data\mid x)f(x) \tag{7}$$

where $f(x)$ is the prior distribution of x, $g(Data\mid x)$ is the likelihood function, and $f(x\mid Data)$ presents the posterior distribution. By using the binomial distribution, the conditional probability of observing r failures in n trials given a PFD, μ, can be presented as follows:

$$g(r\text{ failures in }n\text{ trials}\mid\mu)=\frac{n!}{r!(n-r)!}\mu^r(1-\mu)^{n-r} \tag{8}$$

By integrating equation (8) and equation (6) into Bayes's theorem, which is presented by equation (7), the posterior distribution of μ can be obtained as follows:

$$f(\mu\mid r\text{ failures in }n\text{ trials})=\frac{\tau(a'+b')}{\tau(a')\tau(b')}\mu^{a'-1}(1-\mu)^{b'-1} \tag{9}$$

where $a'=a+r$ and $b'=b+n-r$.

2.3.3. Updating risks by using periodic proof test data

This study assumes that the final safety barrier elements (such as shutdown valves) are subject to continuous aging degradation with time, and periodic proof tests are executed. The degradation process is modeled by a Gamma process and the degradation level $X(t)$ is presented as follows (Zhang et al., 2020):

$$X(t)\sim\Gamma(\alpha t,\beta)=f_{X(t)}(x)=\frac{\beta^{\alpha t}}{\Gamma(\alpha t)}x^{\alpha t-1}e^{-\beta x},\alpha,\beta>0 \tag{10}$$

where $X(0)=0$, the mean and variance of $X(t)$ are $\alpha t/\beta$ and $\alpha t/\beta^2$, respectively. The cumulative density function (CDF) of $X(t)$ for $t>0$ is:

$$F_{X(t)}(x)=\int_0^x f_{X(t)}(x)dx \tag{11}$$

Proof tests are assumed as perfect/no harm tests in this study, which means the proof tests have no direct influence on the degradation process (Gamma process) and only observe/measure the barrier degradation levels. The time spent on tests is also ignored compared to the much longer test intervals. We also assume that the barrier component will fail to play its function when the degradation level reaches or overpasses a predefined failure threshold L. Under those assumptions, the availability of the barrier component in the i-th test interval given the observed degradation level from the (i-1)-th test is as follows:

$$A(t)=Pr\left(X(t)<L\middle|X_{(i-1)\tau}\right)=F_{X(t-(i-1)\tau)}\left(L-X_{(i-1)\tau}\right),(i-1)\tau<t\le i\tau \tag{12}$$

The average PFD of this barrier component in the i-th test interval is calculated as follows.

$$PFD_{avg}^{i}=1-\frac{\int_{(i-1)\tau}^{i\tau}F_{X(t-(i-1)\tau)}\left(L-X_{(i-1)\tau}\right)dt}{\tau},(i-1)\tau<t\le i\tau \tag{13}$$

where PFD_{avg}^{i} is the average PFD of the barrier component. τ is the time interval for proof tests. With the observed degradation level $X_{i\tau}$ becoming available from periodic proof tests continuously, the average PFD of this barrier component at the next time interval can be updated according to Eq (13).

2.3.4. Updating risks by continuous condition monitoring

Condition-monitoring data usually refers to the online-monitoring data that is related to the degradation of target systems of interest (Kim et al., 2015). Condition-monitoring data provides the opportunity to predict and anticipate the failures of target systems with reference to specific thresholds of the monitored variables (Zeng and Zio, 2018). Usually, there are a couple of methods that can be applied for fault detection and diagnosis (FDD), those methods can be classified into model-based FDD and model-free FDD (Zadakbar et al., 2013a). Based on the assumption that the probability of a failure increases as the process moves away further from the normal operation, the probability of a failure can be calculated as follows (Zadakbar et al., 2013a):

$$for\ r>\mu,P=\varphi\left(\frac{r-(\mu+3\sigma)}{\sigma}\right)$$

$$=\int_{-\infty}^{r}\frac{1}{\sqrt{2\pi}\sigma}e^{\frac{-(r-(\mu+3\sigma))^2}{2\sigma^2}}dr \tag{14}$$

$$for\ r<\mu,P=1-\varphi\left(\frac{r-(\mu-3\sigma)}{\sigma}\right)$$

$$=1-\int_{-\infty}^{r}\frac{1}{\sqrt{2\pi}\sigma}e^{\frac{-(r-(\mu-3\sigma))^2}{2\sigma^2}}dr \tag{15}$$

where r is the residual value of the key variable with respect to the system performance, and P is the failure probability of the investigated system. $\mu+3\sigma$ and $\mu-3\sigma$ are the lower and upper threshold for the normal operation, respectively. Additionally, because condition-monitoring data are usually subject to process and observation noises, it is necessary to filter those noises and estimate the true degradation states of process systems with the help of filtering techniques, for instance, Kalman filter (Zadakbar et al., 2013a) and particle filtering (Zeng and Zio, 2018). Because particle filtering (PF) has the capability of being applied to nonlinear and non-Gaussian systems, this study implements the PF for generating residual values of the key variable and estimating the failure probabilities of basic process control systems. A detailed introduction to implementing the PF for residual value (r) generation and fault diagnosis can be found in (Zadakbar et al., 2015). We omit the repeated illustration here.

2.3.5. Consequence assessment

Consequence assessment is another important task of risk assessment. In the SSBM, both quantitative and semi-quantitative risk assessments can be performed and incorporated with the decision-making module for cost-effective decision-making on safety barrier optimization, as shown in Fig. 7. "Consequence" sub-systems take responsibility for consequence assessments in the SSBM. With respect to major accident scenarios, the calculation of disastrous physical effects (associated with fire, explosion, toxic leakage, etc.) and the assessment of their corresponding damages may be integrated to obtain quantitative consequence assessment results. In terms of physical effects modeling, some software (PHAST, ALOHA, Ansys Fluent, FLACS, etc.) based on empirical models or computational fluid dynamics (CFD) models can be employed (Lewis, 2005). Damage analysis models for heat radiation, explosion effects, acute intoxication, and fragments can be found in TNO Green Book (Van Den Bosh et al., 1989) and other studies (Gubinelli et al., 2004; Cozzani et al., 2005).

Due to the compatibility and scalability of the MATLAB/Simulink simulation platform, using blocks from the User-Defined Functions library (Mathworks-User-defined functions., 2022) helps to incorporate

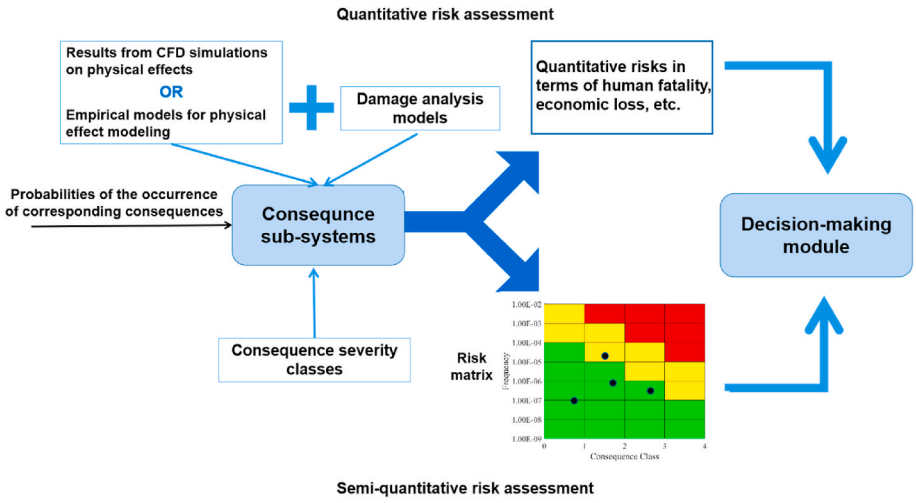


Fig. 7. Conduct consequence assessment based on the "consequence" sub-systems.

physical effect modeling results and damage analysis models. For instance, damage analysis models and empirical models of physical effect modeling can be integrated into the "consequence" sub-systems by using MATLAB code based on the MATLAB Function blocks. It is also possible to input the results from CFD simulations (Cai et al., 2022) into the "consequence" sub-systems and combine them with the damage analysis models to obtain quantitative consequence assessment results. Alternatively, qualitative consequence assessments can also be performed. For instance, the risk matrix is widely used to demonstrate the major accident risks in terms of both probability/frequency and consequence severity. A severity class for typical dangerous phenomena in chemical process industries was suggested by the ARAMIS project (Andersen et al., 2004). If qualitative consequence assessment is performed, the "consequence" sub-systems take the responsibility to collect the occurrence probabilities and severity classes of the corresponding consequences to generate a risk matrix.

2.4. Decision-making on safety barrier improvements (step 3)

This step aims to provide a decision-making module for safety barrier management based on the risk assessment results obtained from step 2. This decision-making module has several functionalities to support safety barrier management. Firstly, it helps to identify critical safety barriers with respect to specific accident consequences through sensitivity analysis. Secondly, the integration of cost-effectiveness analysis (CEA) and optimization algorithms helps decision makers to obtain the optimal cost-effective strategies for safety barrier improvements (such as allocating new barriers and optimizing barrier redundancy structure).

2.4.1. Identify critical safety barriers in terms of risk-reduction

After quantitative or semi-quantitative risk assessment results are obtained by the SSBM, sensitivity analysis may be employed to identify critical safety barriers that object to unacceptable risks. In previous studies, the Birnbaum importance measure (Van der Borst and Schoonakker, 2001), risk reduction measure (Yazdi and Kabir, 2017), and ratio of variance (RoV) measure (Zarei et al., 2017) were used to rank the importance of initiating/intermediate events on the happening of the top event in a fault tree. Similarly, we formulate two measures for ranking the importance/sensitivity of safety barriers on the happening of accident scenarios with unacceptable risks. Using Birnbaum importance measure, the importance of a safety barrier in the occurrence of an unwanted accident scenario is presented as follows:

$$I_n = p_s(p_n = 1) - p_s(p_n = 0) \tag{16}$$

where I_n is the importance of safety barrier n. p_s is the probability of occurrence of the undesired accident scenario. p_n is the probability of failure on demand (PFD) of safety barrier n. Meanwhile, the risk reduction measure of a safety barrier with respect to the happening of an unwanted accident scenario is presented as follows:

$$\mathrm{R}I_n = p_s - p_s(p_n = 0) \tag{17}$$

By ranking the safety barrier criticality based on the above measures and considering the operability of enhancing the corresponding barriers, decision-makers may give more priority to critical barriers for improvements and optimization.

2.4.2. Cost-effective safety barrier optimization

After critical safety barriers are identified, we should investigate the optimal improvement strategies for those barriers. Generally, a series of measures can be implemented to improve the performance of safety barriers, including establishing and allocating new barriers, improving the redundancy structure of safety barriers, revising barrier maintenance intervals, training operators involved in the operation of safety barriers, etc. The specific ways for improving safety barrier performance may be decided based on the real situations of the chemical plants. In the safety science domain, cost-effectiveness analysis (CEA) is widely used to handle the trade-off between cost and safety due to its advantages of conducting comparative studies and its flexibility in determining safety indicators based on the preferences of decision-makers (Reniers and Van Erp, 2016; Chen and Reniers, 2021; Chen et al., 2021). The implementation of CEA in the SSBM helps decision-makers to obtain optimal strategies for safety barrier improvements with the consideration of both economic constraints and technical constraints.

A series of barrier improvement strategies should be formulated before conducting a cost-effectiveness analysis (CEA). Typically, there are two kinds of constraints imposed on decision-makers in terms of CEA. They are i) a minimum acceptable level of effectiveness (Eff_{min}) and ii) a maximum acceptable use of safety budget (Bu_{max}). The optimization problems considering the two kinds of constraints are presented as follows, respectively (Reniers and Van Erp, 2016):

$$\begin{cases} Min(C_i) \\ Eff_i \geq Eff_{min} \\ i \in \{1, 2, 3, \cdots, N\} \end{cases} \tag{18}$$

and

$$\begin{cases} Max(Eff_i) \\ C_i \leq Bu_{max} \\ i \in \{1, 2, 3, \cdots, N\} \end{cases} \tag{19}$$

where i means a strategy i from N possible strategies for improving safety barrier performance. C_i is the cost of implementing strategy i. Eff_i is the effectiveness (risk-reduction performance) of implementing strategy i. In this study, the effectiveness of implementing a strategy is evaluated by a comparison between risk assessment results with and without implementing this strategy. In this way, the effectiveness of implementing a safety barrier optimization strategy can be represented by the corresponding risk-reduction outcomes. If there are only a limited number of strategies can be formulated, the best strategy may be obtained through exhaustive search optimization. Otherwise, evolutionary algorithms (for instance, genetic algorithms) may be implemented to solve the optimization problem with a large solution space.

3. Case study: an application to cost-effective safety barrier optimization

This section demonstrates the application of the proposed approach in dynamic risk assessment and cost-effective safety barrier optimization by using an illustrative case study.

3.1. Scenario building and model configurations

In this study, a continuous stirred tank reactor (CSTR) for carrying out an exothermic first-order reaction A→B was investigated. This CSTR model is adapted from (Pilario and Cao, 2018), in which a jacketed tank is implemented and the reactor temperature T is maintained by manipulating the coolant flow rate Q_c. The dynamic process of the CSTR is simulated by following Eq (20) to Eq (22). The CSTR with its safety barrier systems is shown in Fig. 8.

$$\frac{dC}{dt} = \frac{Q}{V}(C_i - C) - \alpha k C + v_1 \tag{20}$$

$$\frac{dT}{dt} = \frac{Q}{V}(T_i - T) - \alpha\frac{(\Delta H_r)kC}{\rho C_p} - b\frac{UA}{\rho C_p V}(T - T_c) + v_2 \tag{21}$$

$$\frac{dT_c}{dt} = \frac{Q_c}{V_c}(T_{ci} - T_c) + b\frac{UA}{\rho_c C_{pc} V_c}(T - T_c) + v_3 \tag{22}$$

where the inputs of this model are $u = [C_i\ T_i\ T_{ci}]^T$, the outputs are $y = \lfloor C\ T\ T_C\ Q_c \rfloor^T$, v_1, v_2, and v_3 are process noises, and k is an Arrhenius-type rate constant, $k = k_0\ exp\ (\frac{-E}{RT})$. Table 2 shows the parameter values in Eq (20)–Eq (22). In the model, α and b are both equal to 1.00 at normal operating conditions. The CSTR model was developed based on the Simulink platform, and it is available online (Karl, 2022).

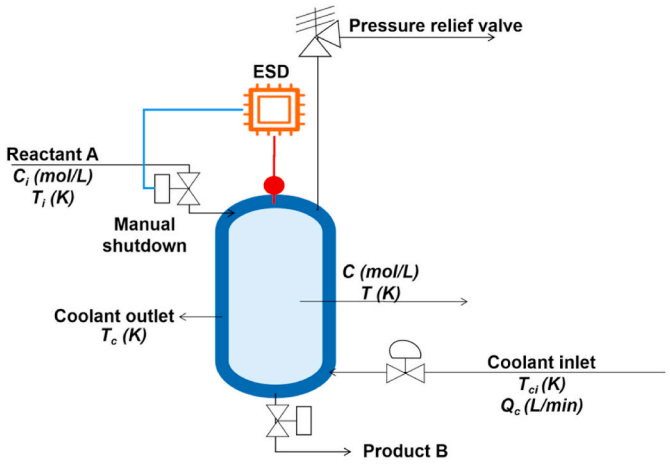


Fig. 8. A continuous stirred tank reactor (CSTR) with its safety barrier systems, adapted from (Pilario and Cao, 2018).

Table 2
Parameter configurations in the CSTR model, adapted from (Pilario and Cao, 2018).

Parameters	Descriptions	Values	Units
Q	Inlet flow rate	100.0	L/min
V	Tank volume	150.0	L
V_c	Jacket volume	10.0	L
ΔH_r	Heat of reaction	-2.0×10^5	cal/mol
UA	Heat transfer coefficient	7.0×10^5	cal/min/K
k_0	Pre-exponential factor to k	7.2×10^{10}	min^{-1}
E/R	Activation energy	1.0×10^4	K
ρ, ρ_c	Fluid density	1000	g/L
C_p, C_{pc}	Fluid heat capacity	1.0	cal/g/K

By following the scenario-building procedures presented in section 2.2, the accident scenarios associated with the CSTR were identified by using the bow-tie technique, and then, the constructed bow-tie was transformed into a Simulink model, as shown in Fig. 9. Meanwhile, the configurations of the initiating events and safety barriers in the Simulink model are illustrated in Table 3. It should be noted that the safety barriers with multiple components in Table 2 all follow an "OR" logic, which means the failure of any one component could lead to the failure of the whole safety barrier.

The probability of cooling system failure is determined and updated based on continuous condition-monitoring data by following the method illustrated in Section 2.3.4. The residual values of ΔT_C (demonstrates the temperature variation inside the cooling jacket) was selected as the variable for failure probability calculation based on Eq (14) and Eq (15). Under ideal operating situations, ΔT_C should be 0 because the temperature inside the cooling jacket remains stable. Therefore, the deviation of the ΔT_C values reflects the likelihood of the cooling system failure. It is assumed that the coolant inlet temperature, coolant outlet temperature, and the temperature inside the reactor (T_{ci}, T_c, T) were monitored. Based on that, particle filtering (PF) was integrated with Eq (22) to generate the residual values of ΔT_C, with the state vector $X = [T_{ci}, T_c, T, \Delta T_C]^T$ and measurement vector $Y = [T_{ci}, T_c, T]^T$. Then, the obtained residual values were integrated into Eq (14) and Eq (15) to estimate the failure probabilities of the cooling system. The normal operation threshold $\pm 3\sigma$ in Eq (14) and Eq (15) is set as $\pm$ 10 according to simulation results under normal operations (as shown in Fig. 11). In real cases, this threshold may be determined based on the real monitored data under normal operating situations with the consultation with experts.

In this study, three ways are used to calculate the PFD of safety barriers/safety barrier components. i) the PFDs can be calculated based on constant failure rates, as presented in Eq (23).

$$PFD = \frac{1}{2}\lambda T \tag{23}$$

where λ is the failure rate of the safety barrier/barrier component, which can be derived from existing databases, such as the OREDA database (OREDA, 2002) and PDS database (Hauge and Onshus, 2010). T is the periodic inspection interval, it is assumed as 4380 h in this study.

ii) In terms of the ESD (emergency shutdown system), constant failure rates were used for the pressure sensor and programmable safety system because the assumption of constant failure rates is usually valid for electronic components (Zhang et al., 2020). By contrast, the degradation of the shutdown valve was considered because it is operated in harsh conditions. The PFD of the shutdown valve was calculated based on the approach presented in Section 2.3.3 and was updated by using periodic proof test data. We used the assumptions and configurations of the shutdown valve from (Zhang et al., 2020), in which the designed closing time for a shutdown valve is 12 s. A predefined failure threshold L was set as 1.25×10^{-3}, and it is assumed that no maintenance

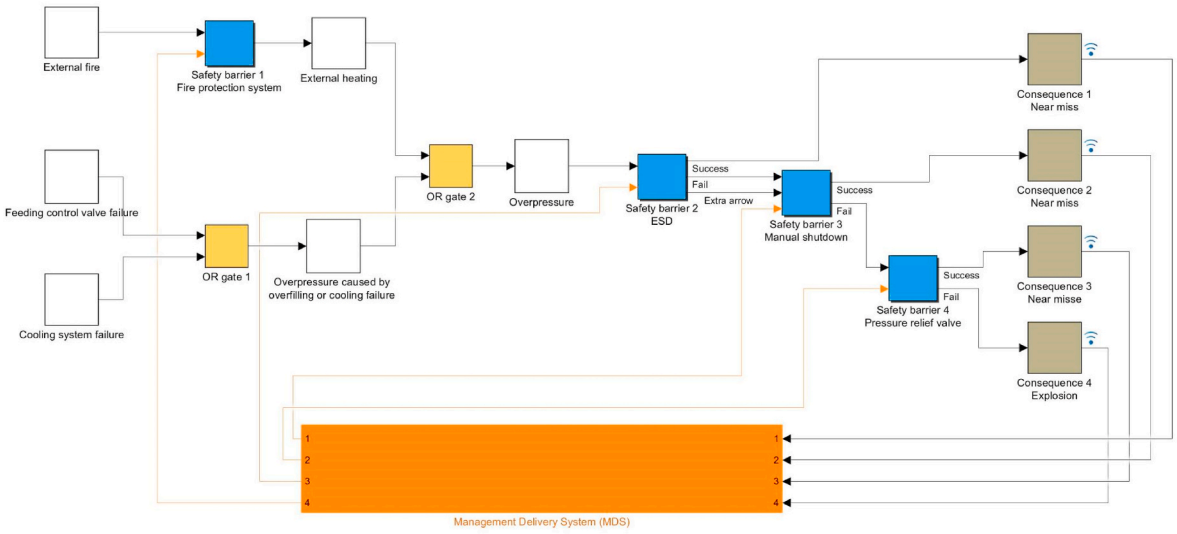


Fig. 9. The developed Simulink model for safety barrier modeling.

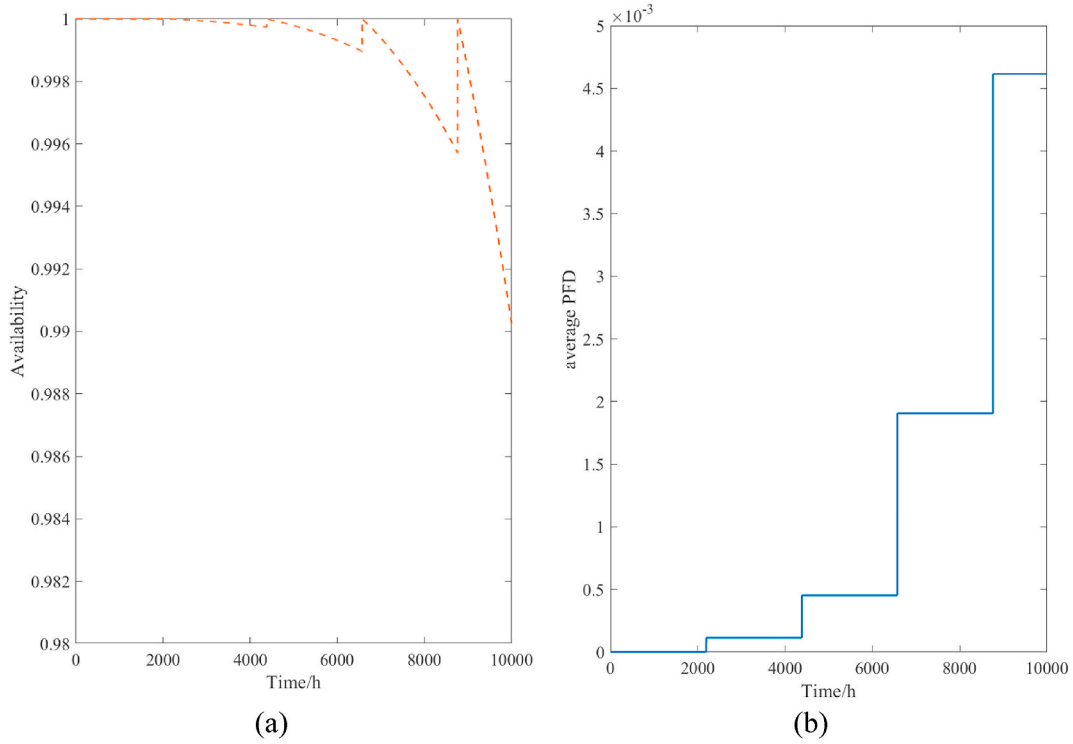


Fig. 10. Availability and average PFDs of the shutdown valve over time.

action will be implemented unless the degradation level exceeds L. α and β used in Eq (10) were set as 1.02×10^{-4} and 1.2×10^{4}, respectively. The time interval for proof tests, τ, is set as 2190 h. By checking the closing time of the shutdown valve and evaluating the corresponding degradation level, the average PFD of the shutdown valve in the test interval can be updated according to Eq (13).

iii) A Beta distribution is used to describe the failure probability of human actions in the manual shutdown barrier. The Beta distribution parameters are set as: a = 32.3 and b = 137.7, adapted from (Roy et al., 2015). As new accident precursor data becomes available, the Beta distribution can be updated through Bayesian updating. Because the ESD barrier and manual shutdown barrier have shared components (a pressure sensor and a shutdown valve), the conditional probability of manual shutdown failure given the failure of ESD is used, according to the method presented in Section 2.2.3.

3.2. Dynamic risk assessment results

This section illustrates the dynamic risk assessment results of the targeted CSTR by integrating periodic proof test data, continuous condition-monitoring data, and accident precursor data into the Simulink-based modeling. The hypothetical accident sequence precursor data of "fail to close valve manually" is given in Table 4. The hypothetical periodic proof test data of the emergency shutdown valve is

Table 3
Configurations of initiating events and safety barriers.

Initiating event OR safety barrier	Descriptions (some safety barriers consist of multiple components)		Configurations of probabilities/PFDs
Initiating event	External fire		probability = 5.52E-02 $\mathbf{y}^{-1}$ (Debray et al., 2004)
Initiating event	Feeding control valve failure		probability = 4.00E-02 $\mathbf{y}^{-1}$ (Taylor, 2010)
Initiating event	Cooling system failure		The probability of cooling system failure is determined and updated by using continuous condition-monitoring data.
Safety barrier	Fire protection system	Smoke/ combustion detector	PFD = 9.02E-03, λ = 4.12E-06 (OREDA, 2002)
		Programmable logic solver	PFD = 2.19E-03, λ = 1.0E-06 (Hauge and Onshus, 2010)
		Fire pump	PFD = 1.58E-01, λ = 7.2E-5 (Gravestock, 2008)
		Deluge Valve	PFD = 1.27E-02, λ = 5.8E-06 (Gravestock, 2008)
Safety barrier	ESD (emergency shutdown system)	Pressure sensor*,[a]	PFD = 3.29E-04, λ = 1.5E-07 (Hauge and Onshus, 2010)
		Programmable safety system	PFD = 2.19E-03, λ = 1.0E-06 (Hauge and Onshus, 2010)
		Shutdown valve*	PFD of the shutdown valve is calculated and updated based on periodic proof test data.
Safety barrier	Manual shutdown	Pressure sensor*	The same as the pressure sensor in ESD.
		Fail to close valve manually	Beta distribution parameters: a = 32.3, b = 137.7, (Roy et al., 2015). The Beta distribution is updated by using accident precursor data.
		Shutdown valve*	The same as the shutdown valve in ESD.
Safety barrier	Pressure relief valve	/	PFD = 2.4E-03, λ = 1.1E-06 (Hauge and Onshus, 2010)

[a] A barrier component with * means it is a shared component.

presented in Table 5. Fig. 10 shows the availability and average PFDs of the shutdown valve over time, which are calculated based on the hypothetical data in Table 5. It is assumed that a shock degradation happened to the cooling system at 5000 h. We simulated this degradation by adding a disturbance following a Gaussian distribution $N(0.01, 0.03)$ to the coolant inlet temperature T_{ci}. It means the degradation reduces the capability and precision of the control system in regulating the key variable at the required level. The residual values of ΔT_C with and without a certain degree of degradation are compared in Fig. 11. The average residual values before and after the degradation were used to calculate the failure probabilities of the cooling system. By employing the periodic proof test data, continuous condition-monitoring data, and accident precursor data for risk profile updating, the dynamic risk profiles of the CSTR explosion accident are obtained and are shown in Fig. 12. The probability distributions obtained from Monte Carlo simulations are demonstrated in (a) and their corresponding mean values are demonstrated in (b). As we can see from Fig. 12, the risk profile increases gradually and peaks at 8760 h, which results from the degradation of the safety barriers and the cooling system.

3.3. Cost-effective barrier optimization

According to the obtained dynamic risk profiles, we demonstrate the risks of CSTR explosion in a risk matrix (Fig. 13), in which the red region means unacceptable, the yellow region means acceptable with mitigation, and the green region means acceptable. Based on the risk profiles at the final stage (8760 h–10000 h), a sensitivity analysis of safety barriers and initiating events were conducted according to section 2.4.1. Two measures (Birnbaum importance measure and risk reduction measure) were used to rank the criticality of safety barriers in risk reduction, as shown in Table 6.

Table 6 shows that the most important safety barriers/barrier components targeting the explosion risk are the pressure sensor, shutdown valve, and pressure relief valve, with importance measures as 1.86E-04,

Table 4
Hypothetical accident sequence precursor data of "fail to close valve manually".

Time (h)	Cumulative failure number	Cumulative trial number
3000	6	30
5000	9	50
7000	11	70

Table 5
Hypothetical periodic proof test data of the shutdown valve.

Test time (h)	Degradation level	Test time (h)	Degradation level
2190	8×10^{-4}	4380	9×10^{-4}
6570	1×10^{-3}	8760	1.1×10^{-3}

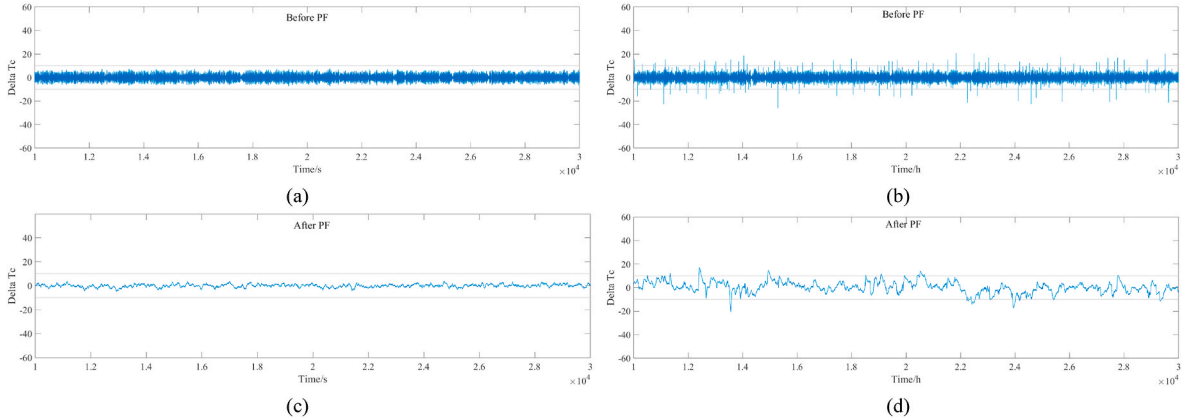


Fig. 11. Residual values of ΔT_C with and without cooling system degradation, (a) without degradation before PF (particle filtering), (b) with degradation before PF (particle filtering), (c) without degradation after PF (particle filtering), and (d) with degradation after PF (particle filtering).

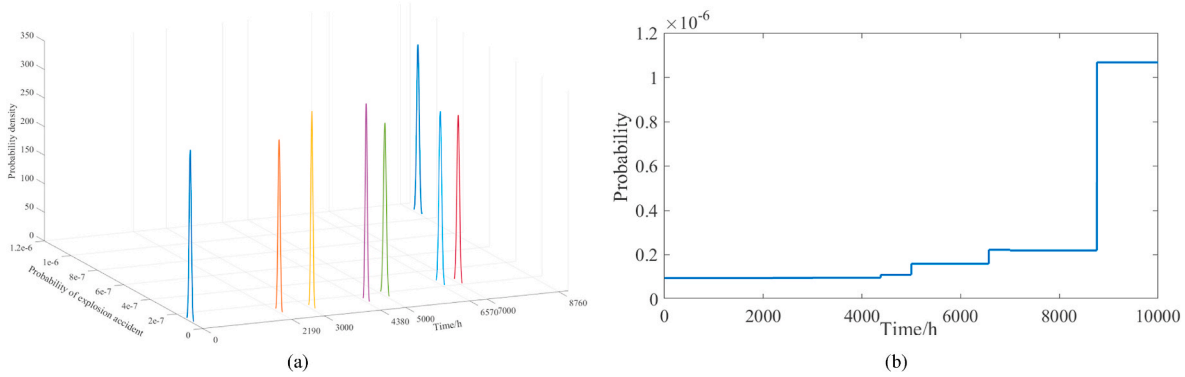


Fig. 12. Risk profiles of the CSTR explosion accident over time, (a) demonstrates the probability distributions obtained from Monte Carlo simulations with 10000 trails (different colors are used to distinguish the probability distributions at different times), and (b) demonstrates the mean values of the probability distributions. (For interpretation of the references to color in this figure legend, the reader is referred to the Web version of this article.)

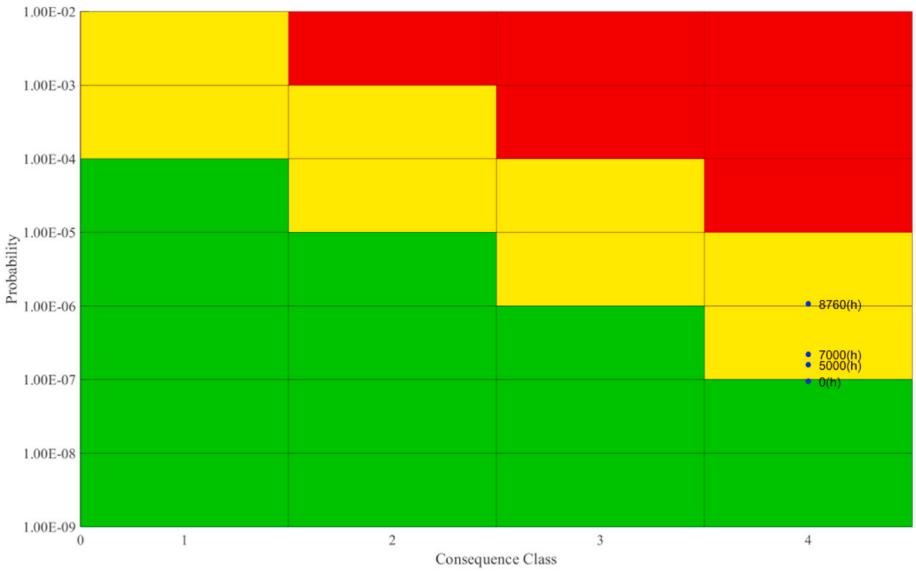


Fig. 13. A risk matrix with respect to time-varied explosion risks.

Table 6
Sensitivity of safety barrier failures and initiating events in the explosion risk.

Safety barrier OR Initiating event	Descriptions	Risk reduction measure	Birnbaum importance measure
Initiating event	External fire	1.28E-07	2.32E-06
Initiating event	Feeding control valve failure	5.38E-07	1.35E-05
Initiating event	Cooling system failure	3.97E-07	1.33E-05
Safety barrier	Fire protection system	1.28E-07	7.20E-07
Safety barrier	ESD Pressure sensor	6.11E-08	1.86E-04
Safety barrier	Shutdown valve	9.32E-07	1.86E-04
Safety barrier	Programmable safety system	9.49E-08	4.33E-05
Safety barrier	Fail to close valve manually	9.49E-08	4.07E-07
Safety barrier	Pressure relief valve	1.09E-06	4.54E-04

1.86E-04, and 4.54E-04, respectively. Considering their current estimated PFDs, the most sensitive safety barriers/barrier components in risk reduction are the pressure relief valve and shutdown valve, with risk reduction measures as 1.09E-06 and 9.32E-07, respectively. Based on the dynamic risk assessment results, the goals for safety barrier management and optimization should be formulated. In this case study, the optimization principles are formulated as follows: i) When the explosion risk exceeds 1.00E-06 y^{-1}, barrier improvements should be made. ii) The goal of safety barrier optimization is to limit the explosion risk below 1.00E-08 y^{-1}. iii) When the degradation of safety barriers or basic process control systems is detected, the maintenance or replacement of the degraded components should be given more priority instead of allocating new safety barriers. In real cases, the safety barrier management/optimization principles may be determined according to the production and safety needs with consultation with experts.

Based on the above optimization principles, the optimization objective function and constraints presented in Eq (18) are adapted for safety barrier optimization. The optimization objective function and constraints are presented as follows:

$$\begin{cases} Min(C_i) \\ Risk_i \le Risk_{threshold} \\ i \in \{1, 2, 3, \cdots, N\} \end{cases} \tag{24}$$

where C_i means the cost of strategy *i*. $Risk_i$ is the risk assessment outcome after implementing strategy *i*. $Risk_{threshold}$ is set as 1.00E-08 y^{-1} in this case study. This optimization aims to minimize the costs spent on safety barrier improvement and meanwhile to ensure the explosion risk is below 1.00E-08 y^{-1}. Because the cooling system degradation and shutdown valve degradation were detected, we considered the

maintenance/replacement of such facilities in all candidate strategies. Apart from that, improvements may be made to the three most important safety barriers/barrier components (pressure sensor, shutdown valve, and pressure relief valve) by adding redundant devices. A series of barrier improvement strategies are formulated, as shown in Table 7. The cost analysis of each strategy is also performed in Table 7.

As shown in Table 7, strategy 4, strategy 6, and strategy 7 are the candidate strategies that meet the optimization constraint, which is to lower the explosion risk below the risk threshold. Among those three strategies, strategy 4 has the lowest total cost (2150€) for safety barrier system improvements, so it is selected as the most cost-effective strategy. For illustrative purposes, seven strategies were formulated, and the results of those strategies were compared to determine the optimal strategy. For more complex systems with more candidate strategies, a similar optimization may be done by comparing the results of those strategies and following exhaustive search optimization. If a large number of strategies can be formulated as candidate strategies, it may become unreasonable to assess all the strategies using exhaustive optimizations. Alternatively, genetic algorithms may be implemented to solve optimization problems with a large solution space. Another study from us demonstrates the application of genetic algorithms in safety barrier optimization (Yuan et al., 2023).

Table 7
Candidate strategies of safety barrier optimization.

Strategy number	Description	Cost analysis	Explosion risk after barrier improvements (y^{-1})
1	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/ replacement).	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); Total cost = a+b = 1400€.	9.2453E-08
2	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/ replacement); c. Add a redundant pressure sensor.	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); c = 600€ (equipment and installation cost)+200€ × 2 (annual maintenance/ inspection cost); Total cost = a+b + c = 2600€.	5.0599E-08
3	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/ replacement); c. Add a redundant shutdown valve.	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); c = 600€ (equipment and installation cost)+200€ × 4 (annual maintenance/ inspection cost); Total cost = a+b + c = 2800€.	9.2452E-08
4	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/ replacement); c. Add a redundant pressure relief valve.	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); c = 450€ (equipment and installation cost)+150€ × 2 (annual maintenance/ inspection cost); Total cost = a+b + c = 2150€.	2.2189E-10
5	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/ replacement); c. Add a redundant pressure sensor; d. Add a redundant shutdown valve.	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); c = 600€ (equipment and installation cost)+200€ × 2 (annual maintenance/ inspection cost); d = 600€ (equipment and installation cost)+200€ × 4 (annual maintenance/ inspection cost); Total cost = a+b + c + d = 3800€.	5.0599E-08
6	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); c = 600€ (equipment and installation cost)+200€ × 2 (annual maintenance/ inspection cost);	1.2144E-10

(continued on next page)

4. Discussions

4.1. A comparison of SSBM and BN

As a widely-used tool for quantitative risk assessment (QRA) and dynamic risk assessment (DRA), Bayesian networks (BN) were also employed to support safety barrier assessment and management. This section compares BN and the proposed SSBM approach considering their characteristics and capabilities in QRA, DRA, and supporting decision-making. It helps practitioners get insight into the application prospects of the SSBM approach. The comparison results are presented in Table 8.

4.2. Recommendations for future work

This study provides a comprehensive tool to support safety barrier management based on dynamic risk assessment results. Periodic proof test data, continuous condition-monitoring data, and accident precursor data are utilized for risk profile updating with the consideration of the degradation of safety barriers and chemical process systems. Our previous study proposed an approach for cost-effective maintenance of safety and security barriers (Yuan et al., 2023), which can serve on the determination of barrier maintenance intervals at the design stage. With the combination of this study, which may be used to make adjustments to barrier maintenance plans and barrier allocation strategies in the operation stage, it is possible to develop a full life cycle safety barrier management system in the future.

However, the imperfection of the proof tests in revealing barrier health states was not considered in this study. In real situations, the proof tests/inspections are usually subject to errors and defects (Zhang et al., 2021). The quantification and modeling of the proof test errors in revealing barrier health states should be further incorporated into the SSBM approach. Additionally, the safety barrier degradation process may be different under different environmental conditions. How to involve environmental influence factors in the estimation of barrier health states may be further investigated.

This study incorporates a model-based fault detection and diagnosis (FDD) approach, which is a preliminary exploration. More advanced FDD methods with more accuracy and adaptability in solving complex non-linear chemical process models may be integrated into the proposed approach for failure estimation of chemical systems. Additionally, dynamic risk assessment was performed by this study through the updating of probabilities while the model structure remains static. In some cases, the model structure may also need to be updated when new evidence

Table 7 (*continued*)

Strategy number	Description	Cost analysis	Explosion risk after barrier improvements (y^{-1})
	replacement); c. Add a redundant pressure sensor; d. Add a redundant pressure relief valve.	c = 450€ (equipment and installation cost)+150€ × 2 (annual maintenance/ inspection cost); Total cost = a+b + c + d = 3150€.	
7	a. Maintenance of the degraded cooling system (restore its performance to the initial); b. Maintenance of the degraded shutdown valve (perfect maintenance/ replacement); c. Add a redundant shutdown valve; d. Add a redundant pressure relief valve.	a = 1000€ (one-time maintenance cost); b = 400€ (replacement cost); d = 600€ (equipment and installation cost)+200€ × 4 (annual maintenance/ inspection cost); c = 450€ (equipment and installation cost)+150€ × 2 (annual maintenance/ inspection cost); Total cost = a+b + c + d = 3550€.	2.2189E-10

Table 8
A comparison of SSBM and BN with respect to safety barrier management.

Approaches	QRA capabilities	DRA capabilities	Decision-making capabilities
BN	BN has the advantage of representing the dependencies of events, incorporating multi-state variables, and updating probabilities in QRA.	Dynamic Bayesian networks (DBN) can be employed for conducting DRA. Hierarchical Bayesian networks can combine with Bayes's theorem to update the reliability of safety barriers and perform DRA (Khakzad et al., 2014).	The combination of BN and influence diagram can be employed to determine the optimal strategy for decision-making (Khakzad, 2021). However, it has difficulties in solving large solution space optimization problems.
SSBM	As a bow-tie-based approach, multiple occurring events (MOE) are not allowed on the left-hand side of the SSBM model. As a result, a simplification should be performed based on the minimal cut sets to determine the correct model structure. SSBM highlights deliberately inserted safety barrier. Its relative simplicity supports communication with non-expert stakeholders and facilitates safety barrier audition and management.	Due to the flexibility and compatibility of the Simulink simulations, SSBM is able to incorporate the data from various sources (periodic proof test data, continuous condition-monitoring data, accident precursor data, etc.) to update the failure probabilities of safety barriers and also update the happening probabilities of initiating events.	SSBM has the advantage of integrating with various optimization algorithms (exhaustive search algorithms, evolutionary algorithms, etc.) to solve large solution space optimization problems and support decision-making.

becomes available. The capability of the SSBM in model structure updating may be enhanced. The case study in this paper only demonstrates the application of the SSBM in qualitative consequence assessment by using a risk matrix. The feasibility of the SSBM in quantitative consequence assessment with the integration of physical effects modeling and damage analysis models should be further validated.

5. Conclusions

This study proposes an integrated approach to facilitate dynamic risk-informed safety barrier management. A simulation tool, which is named Simulink-based safety barrier modeling (SSBM), is developed to integrate dynamic risk assessment and safety barrier management in chemical process industries. The SSBM contains multiple functionalities to support decision-making on safety barrier optimization based on evaluating the risk-reduction performance of safety barriers. Periodic proof test data, continuous condition-monitoring data, and accident precursor data are combined to update risk profiles with the consideration of safety barrier degradation. The combination of cost-effectiveness analysis (CEA) and optimization algorithms is employed by the SSBM to determine the optimal strategies for safety barrier establishments and improvements from a cost-effectiveness perspective. A dynamic risk assessment of a continuous stirred tank reactor (CSTR) was employed as the case study to validate the feasibility of the proposed approach in dynamic risk-informed safety barrier management. The results show that the pressure relief valve and shutdown valve are the most critical safety barrier/barrier components for risk reduction. Apart from implementing maintenance/replacement of the degraded facilities, the allocation of a redundant pressure relief valve is the most cost-effective strategy for improving the safety barrier system. A comparison of the SSBM and Bayesian networks is given to demonstrate the characteristics and capabilities of the SSBM in risk assessment and safety barrier management. The comparison shows that the SSBM has advantages in supporting communication with non-expert stakeholders, and various techniques/methods can be incorporated into the SSBM to facilitate safety barrier assessment and risk-based safety barrier management due to the flexibility and adaptability of the Matlab/Simulink platform.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors are unable or have chosen not to specify which data has been used.

Acknowledgments

This work is supported by the China Scholarship Council (Grant No: 202006430007).

References

Andersen, H., Casal, J., Dandrieux, A., Debray, B., De Dianous, V., Duijm, N., Gowland, R., 2004. ARAMIS User Guide. *EC Contract Number EVG1-CT-2001-00036*.
Andrews, J.D., Dunnett, S.J., 2000. Event-tree analysis using binary decision diagrams. IEEE Trans. Reliab. 49 (2), 230–238.
Cai, J., Wu, J., Yuan, S., Kong, D., Zhang, X., 2022. Prediction of gas leakage and dispersion in utility tunnels based on CFD-EnKF coupling model: A 3D full-scale application. Sustainable Cities and Society 80, 103789.
CCPS, 2001. Layers of Protection Analysis: Simplified Process Risk Assessment. American Institute of Chemical Engineers-Center of Chemical Process Safety, New York.
CCPS/EI, 2018. Bow Ties in Risk Management. Center for Chemical Process Safety and Energy Institute (UK), Wiley - AIChE, New York.

Chaturvedi, D.K., 2017. Modeling and Simulation of Systems Using MATLAB® and Simulink®. CRC press.
Chen, C., Reniers, G., 2021. Economic model for tackling intentional domino effects in a chemical facility. In: Dynamic Risk Assessment and Management of Domino Effects and Cascading Events in the Process Industry. Elsevier, pp. 193–222.
Chen, C., Reniers, G., Khakzad, N., Yang, M., 2021. Operational safety economics: foundations, current approaches and paths for future research. Saf. Sci. 141, 105326.
Cozzani, V., Gubinelli, G., Antonioni, G., Spadoni, G., Zanelli, S., 2005. The assessment of risk caused by domino effect in quantitative area risk analysis. J. Hazard Mater. 127 (1–3), 14–30.
Debray, B., Piatyszek, E., Cauffet, F., Londiche, H., 2004. Frequencies and Probabilities Data for the Fault Tree. Accidental Risk Assessment Methodology for Industries in the Framework of SEVESO II Directive (ARAMIS), Armines, vol. 100. École Nationale Supérieure de Mines de Saint Etienne, France.
Dimaio, F., Scapinello, O., Zio, E., Ciarapica, C., Cincotta, S., Crivellari, A., et al., 2021. Accounting for safety barriers degradation in the risk assessment of oil and gas systems by multistate Bayesian networks. Reliab. Eng. Syst. Saf. 216, 107943.
Duijm, N.J., 2009. Safety-barrier diagrams as a safety management tool. Reliab. Eng. Syst. Saf. 94 (2), 332–341.
Eide, S.A., Wierman, T.E., Gentillon, C.D., Rasmuson, D.M., Atwood, C.L., 2007. Industry-average Performance for Components and Initiating Events at US Commercial Nuclear Power Plants. NUREG/CR-6928; Nuclear Regulatory Commission, Washington, DC, USA.
Gibson, J.J., 1961. The contribution of experimental psychology to the formulation of the problem of safety–a brief for basic research. Behavioral approaches to accident research 1 (61), 77–89.
Gravestock, N., 2008. Effectiveness of Fire Safety Systems for Use in Quantitative Risk Assessments. New Zealand Fire Service Commission, *Wellington,* NZ.
Gubinelli, G., Zanelli, S., Cozzani, V., 2004. A simplified model for the assessment of the impact probability of fragments. J. Hazard Mater. 116 (3), 175–187.
Haasl, D.F., Roberts, N.H., Vesely, W.E., Goldberg, F.F., 1981. Fault Tree Handbook (No. NUREG-0492). Nuclear Regulatory Commission. Office of Nuclear Regulatory Research, Washington, DC (USA).
Hauge, S., Onshus, T., 2010. Reliability Data for Safety Instrumented Systems PDS Data Handbook, 2010 Edition. SINTEF Report A, 13502.
Hauptmanns, U., 2002. Analytical propagation of uncertainties through fault trees. Reliab. Eng. Syst. Saf. 76 (3), 327–329.
Hickman, J.W., 1983. PRA Procedures Guide: a Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, vol. 2300. NUREG/CR.
Johansen, I.L., Rausand, M., 2015. Barrier management in the offshore oil and gas industry. J. Loss Prev. Process. Ind. 34, 49–55.
Kalantarnia, M., Khan, F., Hawboldt, K., 2009. Dynamic risk assessment using failure assessment and Bayesian theory. J. Loss Prev. Process. Ind. 22 (5), 600–606.
Kalantarnia, M., Khan, F., Hawboldt, K., 2010. Modelling of BP Texas City refinery accident using dynamic risk assessment approach. Process Saf. Environ. Protect. 88 (3), 191–199.
Karl, Ezra Pilario, 2022. Feedback-controlled CSTR process for fault simulation. In: MATLAB Central File Exchange. Retrieved. https://www.mathworks.com/matlabcentral/fileexchange/66189-feedback-controlled-cstr-process-for-fault-simulation. (Accessed 3 November 2022).
Khakzad, N., 2021. Optimal firefighting to prevent domino effects: methodologies based on dynamic influence diagram and mathematical programming. Reliab. Eng. Syst. Saf. 212, 107577.
Khakzad, N., Khan, F., Amyotte, P., 2012. Dynamic risk analysis using bow-tie approach. Reliab. Eng. Syst. Saf. 104, 36–44.
Khakzad, N., Khan, F., Paltrinieri, N., 2014. On the application of near accident data to risk analysis of major accidents. Reliab. Eng. Syst. Saf. 126, 116–125.
Khakzad, N., Landucci, G., Reniers, G., 2017. Application of dynamic Bayesian network to performance assessment of fire protection systems during domino effects. Reliab. Eng. Syst. Saf. 167, 232–247.
Kim, H., Lee, S.H., Park, J.S., Kim, H., Chang, Y.S., Heo, G., 2015. Reliability data update using condition monitoring and prognostics in probabilistic safety assessment. Nucl. Eng. Technol. 47 (2), 204–211.
Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab. Eng. Syst. Saf. 143, 30–43.
Latif-Shabgahi, G., Tajarrod, F., 2009. A new approach for the construction of fault trees from system simulink. In: International Conference on Availability, Reliability and Security, vol. 2009. IEEE, pp. 712–717.
Lewis, S., 2005. An overview of leading software tools for QRA. American Society of Safety Engineers–Middle East, pp. 18–22.
Manno, G., Chiacchio, F., Compagno, L., D'Urso, D., Trapani, N., 2012. MatCarloRe: an integrated FT and Monte Carlo Simulink tool for the reliability assessment of dynamic fault tree. Expert Syst. Appl. 39 (12), 10334–10342.
Mathworks-User-defined functions. (n.d.). Retrieved October 14, 2022, from https://nl.mathworks.com/help/simulink/user-defined-functions.html.
Meel, A., Seider, W.D., 2006. Plant-specific dynamic failure assessment using Bayesian theory. Chem. Eng. Sci. 61 (21), 7036–7056.
Misuri, A., Landucci, G., Cozzani, V., 2020. Assessment of safety barrier performance in Natech scenarios. Reliab. Eng. Syst. Saf. 193, 106597.
Misuri, A., Landucci, G., Cozzani, V., 2021. Assessment of risk modification due to safety barrier performance degradation in Natech events. Reliab. Eng. Syst. Saf. 212, 107634.
OREDA, 2002. Offshore Reliability Data Handbook. Trondheim, Norway: DNV.
Ouache, R., Kabir, M.N., Adham, A.A., 2015. A reliability model for safety instrumented system. Saf. Sci. 80, 264–273.
Papadopoulos, Y., Maruhn, M., 2001. Model-based synthesis of fault trees from matlab-simulink models. In: 2001 International Conference on Dependable Systems and Networks. IEEE, pp. 77–82.
Pilario, K.E.S., Cao, Y., 2018. Canonical variate dissimilarity analysis for process incipient fault detection. IEEE Trans. Ind. Inf. 14 (12), 5308–5315.
Pitblado, R., Fisher, M., Nelson, B., Fløtaker, H., Molazemi, K., Stokke, A., 2016. Concepts for dynamic barrier management. J. Loss Prev. Process. Ind. 43, 741–746.
Reason, J., Hollnagel, E., Paries, J., 2006. Revisiting the Swiss cheese model of accidents. J. Clin. Eng. 27 (4), 110–115.
Reniers, G.L., Van Erp, H.N., 2016. Operational Safety Economics: a Practical Approach Focused on the Chemical and Process Industries. John Wiley & Sons.
Roy, A., Srivastava, P., Sinha, S., 2015. Dynamic failure assessment of an ammonia storage unit: a case study. Process Saf. Environ. Protect. 94, 385–401.
Schmitz, P., Swuste, P., Reniers, G., van Nunen, K., 2020. Mechanical integrity of process installations: barrier alarm management based on bowties. Process Saf. Environ. Protect. 138, 139–147.
Schmitz, P., Swuste, P., Reniers, G., van Nunen, K., 2021. Predicting major accidents in the process industry based on the barrier status at scenario level: a practical approach. J. Loss Prev. Process. Ind. 71, 104519.
Siu, N.O., Kelly, D.L., 1998. Bayesian parameter estimation in probabilistic risk assessment. Reliab. Eng. Syst. Saf. 62 (1–2), 89–116.
Taylor, J.R., 2010. The QRAQ Project Volume 4: Frequency of Releases and Accidents (accessible 2022, May). https://www.academia.edu/35376294/The_QRAQ_Project_Volume_4_Frequency_of_Releases_and_Accidents.
Van Den Bosh, C.J.H., Merx, W.P.M., Jansen, C.M.A., De Weger, D., Reuzel, P.G.J., Leeuwen, D.V., Blom-Bruggerman, J.M., 1989. Methods for the Calculation of Possible Damage (Green Book). The Hague (NL): Committee for the Prevention of Disasters.
Van der Borst, M., Schoonakker, H., 2001. An overview of PSA importance measures. Reliab. Eng. Syst. Saf. 72 (3), 241–245.
Wu, S., Li, B., Zhou, Y., Chen, M., Liu, Y., Zhang, L., 2022. Hybrid Dynamic Bayesian network method for performance analysis of safety barriers considering multi-maintenance strategies. Eng. Appl. Artif. Intell. 109, 104624.
Yazdi, M., Kabir, S., 2017. A fuzzy Bayesian network approach for risk analysis in process industries. Process Saf. Environ. Protect. 111, 507–519.
Yazdi, M., Kabir, S., Walker, M., 2019. Uncertainty handling in fault tree based risk assessment: state of the art and future perspectives. Process Saf. Environ. Protect. 131, 89–104.
Yuan, S., Yang, M., Reniers, G., Chen, C., Wu, J., 2022a. Safety barriers in the chemical process industries: a state-of-the-art review on their classification, assessment, and management. Saf. Sci. 148, 105647.
Yuan, S., Cai, J., Reniers, G., Yang, M., Chen, C., Wu, J., 2022b. Safety barrier performance assessment by integrating computational fluid dynamics and evacuation modeling for toxic gas leakage scenarios. Reliab. Eng. Syst. Saf. 226, 108719.
Yuan, S., Yang, M., Reniers, G., Chen, C., 2022c. An approach for identification of integrated safety and security barriers in the chemical process industries. Chem. Eng. Transact. 90, 571–576.
Yuan, S., Reniers, G., Yang, M., Bai, Y., 2023. Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm. Process Saf. Environ. Protect. 170, 356–371.
Zadakbar, O., Imtiaz, S., Khan, F., 2013a. Dynamic risk assessment and fault detection using a multivariate technique. Process Saf. Prog. 32 (4), 365–375.
Zadakbar, O., Imtiaz, S., Khan, F., 2013b. Dynamic risk assessment and fault detection using principal component analysis. Ind. Eng. Chem. Res. 52 (2), 809–816.
Zadakbar, O., Khan, F., Imtiaz, S., 2015. Dynamic risk assessment of a nonlinear non-Gaussian system using a particle filter and detailed consequence analysis. Can. J. Chem. Eng. 93 (7), 1201–1211.
Zarei, E., Azadeh, A., Khakzad, N., Aliabadi, M.M., Mohammadfam, I., 2017. Dynamic safety assessment of natural gas stations using Bayesian network. J. Hazard Mater. 321, 830–840.
Zeng, Z., Zio, E., 2018. Dynamic risk assessment based on statistical failure data and condition-monitoring degradation data. IEEE Trans. Reliab. 67 (2), 609–622.
Zeng, T., Chen, G., Yang, Y., Chen, P., Reniers, G., 2020. Developing an advanced dynamic risk analysis method for fire-related domino effects. Process Saf. Environ. Protect. 134, 149–160.
Zhang, A., Liu, Y., 2022. Performance evaluation of digitalized safety barriers. In: Methods in Chemical Process Safety, vol. 6. Elsevier, pp. 281–307.
Zhang, A., Zhang, T., Barros, A., Liu, Y., 2020. Optimization of maintenances following proof tests for the final element of a safety-instrumented system. Reliab. Eng. Syst. Saf. 196, 106779.
Zhang, A., Srivastav, H., Barros, A., Liu, Y., 2021. Study of testing and maintenance strategies for redundant final elements in SIS with imperfect detection of degraded state. Reliab. Eng. Syst. Saf. 209, 107393.