Process Safety and Environmental Protection 170 (2023) 356–371

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

journal homepage: www.journals.elsevier.com/process-safety-and-environmental-protection

Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm

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

[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
[f] School of Emergency Management & Safety Engineering, China University of Mining and Technology, Beijing 100083, China

ARTICLE INFO

Keywords:
Barrier maintenance
Cost-effectiveness analysis
Integration of safety and security
Barrier modeling
Genetic algorithm
Chemical industry

ABSTRACT

Chemical plants face safety hazards and security threats that may induce catastrophic scenarios. Safety and security barriers are employed widely to protect chemical plants from accidental and intentional undesired events and mitigate consequences. Managing safety and security barriers effectively and economically is a research topic with practical significance. The analysis of undesired event scenarios, including both accidental and intentional adverse scenarios, and assessing associated safety and security barriers are critical regarding cost-efficient barrier maintenance. This study proposes a novel approach for optimizing safety and security barrier maintenance strategy considering economic constraints. This approach consists of three steps: scenario building and barrier identification, barrier modeling, and determining optimal barrier maintenance intervals. In the proposed approach, accident scenarios in terms of safety and physical security are constructed using the extended bow-tie diagrams. After associated safety and security barriers are identified, a system simulation model is developed to conduct barrier modeling based on MATLAB/Simulink simulations, in which the barrier maintenance, the impacts of human and organizational barriers, and the correlations between barriers caused by shared components are considered. Finally, a combination of cost-effectiveness analysis (CEA) and genetic algorithm (GA) is employed to support the decision-making on barrier maintenance optimization. An illustrative case is employed in this study to validate the feasibility of the proposed approach.

1. Introduction

Safety and security barriers are implemented in various forms (e.g., technical and non-technical) to protect chemical plants from undesired events in terms of prevention and mitigation of potentially catastrophic consequences (Zeng et al., 2020; Yuan et al., 2022c). Remarkably, because events caused by intentional and malevolent acts may induce catastrophic accidents, integrating safety and security barriers during the risk management process is strongly recommended (Yuan et al., 2022b). The integration of safety and security and the safety and security risk co-analysis of chemical plants have already been investigated in previous studies. For example, integrated safety and security risk assessments were recommended considering the interaction among safety and security-related causal factors through a dynamic risk assessment approach (Song et al., 2019a, 2019b). An approach based on dynamic graphs was proposed to integrate safety and security resources to reduce the risk of intentional domino effects (Chen et al., 2019). Iaiani et al. (2022) investigated the identification of reference scenarios associated with security attacks on the process industries using reference Bow-Ties. Additionally, an integrated safety and security analysis for cyber-physical systems (CPS) has also been studied, considering harmful physical scenarios induced by cyber-attacks (Yang et al., 2021; Guzman et al., 2021). The motivations for integrated management of safety and security (IMSS) and the current state of IMSS in Seveso plants were investigated by (Ylönen et al., 2022). The results show that despite the ongoing development in IMSS at chemical plants and chemical industrial sites, IMSS is still in its infancy. Risk sources, including both safety hazards and malicious acts that could lead to undesired harm scenarios,

* Corresponding author.
** Corresponding author at: Safety and Security Science Section, Faculty of Technology, Policy and Management, TU Delft, Delft, the Netherlands.
E-mail addresses: S.Yuan-2@tudelft.nl (S. Yuan), G.L.L.M.E.Reniers@tudelft.nl (G. Reniers).

https://doi.org/10.1016/j.psep.2022.12.008
Received 3 September 2022; Received in revised form 26 November 2022; Accepted 4 December 2022
Available online 9 December 2022

should be investigated in the identification of the hazardous scenarios and also in the barrier management process. However, integrated management of safety and security barriers is still challenging, particularly in the use of quantitative risk assessment to support barrier management.

Quantitative barrier assessment and further barrier management are lacking regarding security risk analysis. By contrast, applying the barrier concept in the safety science domain has a more extended history. The approaches and strategies for safety barriers assessment and management were already investigated by researchers from different institutions (Johansen and Rausand, 2015; Landucci et al., 2015; Schmitz et al., 2020; Hosseinnia Davatgar et al., 2021; Yuan et al., 2022a; Wu et al., 2022). Typically, the bow-tie diagram was widely used and recommended in the performance assessment and management of safety barriers due to its advantages in being capable of quantitative analysis and relatively straightforward. QRA (quantitative risk assessment) is highly suggested to support safety barrier management by researchers (Pitblado et al., 2016; Bucelli et al., 2017; Yuan et al., 2022c). The ARAMIS (Accidental Risk Assessment Methodology for Industries) project integrated add-on safety barriers into a QRA framework to facilitate safety barrier management with respect to major accident scenarios (Andersen et al., 2004; De Dianous and Fievez, 2006). The I-RISK project took into account the performance of hardware and humans to conduct risk assessments of LOC (loss of containment) by evaluating the technical model, the management model, and their interface (Papazoglou et al., 2003). CCPS (USA) and Energy Institute (UK) developed guidance on how bow-tie diagrams can be employed for risk management through the compelling depiction of safety barriers (CCPS/EI, 2018). Additionally, an extension of bow-tie diagrams to the security risk analysis or safety and security (in one go) risk analysis was also investigated in previous studies (Abdo et al., 2018; Bernsmed et al., 2017; Ji et al., 2021), which demonstrates bow-tie diagrams have the potential to facilitate integrated safety and security risk management and barrier management.

Regarding barrier maintenance and management, barrier aging, degradation, and the influence of human and organizational factors should be considered (Fiorentini and Marmo, 2018; CCPS/EI, 2018). Generally, there are sorts of approaches widely-used for chemical process facility maintenance, for instance, reliability centered maintenance (RCM) (Eisinger and Rakowsky, 2001), condition-based maintenance (CBM) (Wang et al., 2022), preventive maintenance (PM) (Basri et al., 2017), risk based inspection (RBI) (Tan et al., 2011), or a combination of them. The objective of facility maintenance is to maximize the availability and efficiency of the facility and guarantee a safe and correct operation and minimize costs. Because the common goal of safety barriers and security barriers is to control risk, risk-based approaches are suitable for supporting safety and security barrier maintenance considering risk sources, including both safety hazards and malicious acts. By implementing the integration of barrier maintenance and QRA, the effectiveness of barrier maintenance is reflected by risk reduction in terms of specific accident scenarios. Then, barrier maintenance can be planned based on quantitative barrier importance to risk control in a manner similar to risk based inspection (RBI) (Pitblado et al., 2016).

Previous studies investigated the interaction among safety and security-related causal factors in risk assessment (Song et al., 2019a, 2019b). Because barriers are important elements that influence risk propagation in risk assessment, the interactions and correlations between barriers cannot be ignored. Barriers usually have synergistic effects on the risk reduction of undesired accident scenarios, for instance, safety barriers work on controlling safety risks, while security barriers prevent malicious acts and further reduce malicious acts-induced safety risks as well. Therefore, the development of an integrated risk analysis model considering the interventions of both safety barriers and security barriers is necessary. Additionally, if two barriers have a shared component/element, their failure probabilities are correlated and further their effects on risk reduction become correlated. For instance, an automatic emergency shutdown system (ESD) and a manual shutdown may use the same physical shutdown valve. Thus, the failure probabilities of ESD and manual shutdown are correlated and influenced by the performance of the shared shutdown valve. Therefore, it's necessary to consider the correlations between barriers caused by the shared components/elements to facilitate more rational decision-making.

Meanwhile, the economic issues of barrier maintenance play an indispensable role in the decision-making process for safety and security management since companies usually face budget limitations. The trade-off between accident risk levels and barrier maintenance costs is vital concerning cost-efficient barrier maintenance (Zhen et al., 2021). To tackle the problems in the trade-off between accident risks and barrier investment, the integration of QRA and cost-effectiveness analysis (CEA) helps to support the decision-making on safety and security barrier management (Chen and Reniers, 2021). However, for a complex system with many safety and security barriers, it is difficult to determine a specific optimal strategy with the consideration of the maintenance interval of each barrier because the solution space is much large. Targeting this challenge, the implementation of evolutionary algorithms (such as genetic algorithms) instead of exhaustive searching has the potential to determine the optimal strategy under a large solution space.

Based on the above discussions, we identified several gaps in terms of cost-effective safety and security barrier maintenance as follows.

i) An integrated quantitative risk analysis model with the consideration of both safety and security risk sources and the correlation/dependency between barriers is needed.
ii) The integration of QRA and barrier maintenance optimization should be achieved.
iii) New approaches should be developed to obtain the optimal barrier maintenance strategy with the consideration of the maintenance interval of each barrier (with a large solution space) from a cost-effective perspective.

Targeting the challenges in integrated safety and security risk assessment and cost-effective barrier maintenance, this study extends bow-tie diagrams for safety and security analysis of chemical process control systems. A novel approach is proposed to conduct risk assessments of accident scenarios considering both safety and security barriers and their correlations and further support cost-effective decision-making on barrier maintenance. The remainder of this paper is organized as follows. Firstly, the methodologies developed for cost-effective barrier maintenance are described in Section 2. Then, a system simulation tool is proposed for barrier modeling and facilitating barrier optimization in Section 3. Section 4 demonstrates the application of the proposed approach by using an illustrative case study. The discussion on the novelty of the proposed approach and the recommendations for future work are given in Section 5. Finally, conclusions are presented in Section 6.

2. Methodology

This section describes the overall framework of the methodology first, followed by detailed descriptions of each step of the methodology.

2.1. Overall framework

To address the current gaps in cost-effective safety and security barrier maintenance, several main principles are proposed as follows. i) Both safety and security risk sources should be identified and depicted in the scenario building phase, meanwhile, the interventions of safety and security barriers should also be investigated with the consideration of their correlations/dependencies. ii) The effectiveness of allocating barriers and also implementing barrier maintenance strategies should be measured by their corresponding risk-reduction performance in terms of specific accident scenarios. Thus, an integrated QRA model for safety

and security risk analysis is necessary. iii) The maintenance interval/strategy of each barrier should be optimized based on the risk-reduction performance of such barriers from a systemic and cost-effective perspective. It means that the barrier maintenance strategy should be optimized based on the synergistic effects of barriers on system risk reduction, rather than evaluating and optimizing each barrier according to its own probability of failure and consequence of failure.

Based on the above principles, a novel approach with three steps (scenario building & barrier identification, barrier modeling, and optimization of barrier maintenance strategy) is proposed, as shown in Fig. 1. The first step aims to build accident scenarios in terms of both safety and security and identify the scenario-associated barriers, for example, by using bow-tie diagrams. Then, the performance assessment of barriers should be conducted in step 2 by a barrier modeling with the consideration of technical barrier maintenance, human and organizational barriers, and the correlation/dependency between barriers. The performance of barriers in terms of risk-reduction of specific accident scenarios is reflected by comparing the risk assessment results. Finally, with the combination of CEA and optimization algorithms (such as genetic algorithms), step 3 aims to support decision-making on barrier maintenance strategy concerning the trade-off between accident risks and barrier maintenance costs. A detailed illustration of the three steps is presented in the following sub-sections.

2.2. Scenario building & barrier identification (step 1)

Bow-tie identification techniques are widely used for HAZard IDentification (HAZID) and safety risk management (de Ruijter and Guldenmund, 2016), for instance, the MIMAH (methodology for identifying major accident hazards) (Andersen et al., 2004) and DyPAS (Dynamic Procedure for Atypical Scenarios Identification) (Paltrinieri et al., 2013). Bow-tie techniques also have the potential to identify and visualize accident scenarios in terms of safety, physical security, and cyber security (Abdo et al., 2018; Ji et al., 2021). In this study, bow-tie diagrams are employed to identify and visualize accident scenarios in terms of both safety hazards and security threats. Safety and security barriers can be identified and located on the bow-tie diagrams with the help of existing documents or databases related to the investigated process control systems. For example, a database of checklists is available to support the barrier identification of CPSs (Guzman et al., 2021). For a series of barriers following an AND logic gate, formula (1) is used to calculate the output probability. For a series of barriers following an OR logic gate, formula (2) can be applied.

$$P_{OUT} = P_{IN} * (PFD_1 * PFD_2 \cdots PFD_n) \tag{1}$$

$$P_{OUT} = P_{IN} * (1 - (1 - PFD_1) * (1 - PFD_2) \cdots (1 - PFD_n)) \tag{2}$$

where P_{OUT} is the output probability and P_{IN} is the input probability of the branch. PFD_1 to PFD_n indicate the PFDs of barriers, and n is the number of barriers. For a barrier with two outlet branches, one branch presents the failing of the barrier with a probability(PFD). Another presents the barrier succeeding with a probability that is 1-PFD.

2.3. Barrier modeling (step 2)

The performance of implementing a barrier can be reflected by the risk reduction of specific accident scenarios under the protection of this barrier (Schmitz et al., 2021). The probability of failure on demand (PFD) is widely used to describe the unavailability of barriers that can be calculated based on the failure rates of the barrier components. This section elaborates on how to determine PFDs of barriers and assess the performance of barriers through a dynamic barrier modeling approach.

2.3.1. PFD calculation considering barrier maintenance

For a barrier constituted by multiple components, fault tree analysis is used to calculate the PFD of this barrier and then the calculated PFD is used for probabilistic risk assessment. The unavailability/failure probability of a technical barrier was considered following the exponential distribution and can be expressed as a function of time in previous studies (IEC, 2016; Redutskiy, 2017; Schmitz et al., 2021; Wu et al., 2022). This assumption is used to describe the unavailability of technical barriers/barrier components in this study. For simplification purposes, PFD can be calculated according to formula (3), in which a constant failure rate is assumed to calculate the cumulative failure probability of the barrier.

$$PFD_{withoutBM}(t) = 1 - e^{-\lambda t} \tag{3}$$

where λ is the barrier failure rate and t denotes time. Some failure rate databases for safety barriers or the technical components of safety barriers are available and can be retrieved from (OREDA, 2002; Ottermo et al., 2021). In this study, it is assumed that the performance of a barrier can restore to its original state after the barrier maintenance, which can be called complete functional maintenance/test (Ottermo et al., 2021). We assume that the barrier failure rate will not change after complete functional maintenance, but it may not be equal to the original value in practice. We assume that the performance of a barrier follows a linear distribution during the maintenance period. If barrier maintenance with a time interval of T is conducted, the *PFD* of this barrier/barrier component can be calculated according to formula (4), which is a periodic piecewise function composed of exponential distributions and linear distributions. The starting times of barrier maintenance are the piecewise points.

$$PFD_{withBM}(t) = \begin{Bmatrix} 1 - e^{-\lambda * (t\%(T+h))}, n(T+h) \le t < (n+1)T + nh \\ 1 - e^{-\lambda T} - (1 - e^{-\lambda T})/h * (t\%(T+h) - T), (n+1)T + nh \le t < (n+1)(T+h) \end{Bmatrix} \tag{4}$$

where h is the required maintenance time. $t\%(T+h)$ means the remainder when dividing t by $T + h$. n is an integer from 0 to positive infinity. A comparison between the time-dependent PFD of a barrier using different maintenance intervals is shown in Fig. 2.

2.3.2. Human and organizational barriers

The need to involve human error probability (HEP) in the quantification of PFDs of the safety instruments executed by humans was suggested (Hauge et al., 2010). For the barrier systems involving human actions, the PFD of the whole barrier can be calculated by using the PFD of each barrier component/element according to the logical architecture comprised of technical components and human actions. HEP can be estimated by Human Reliability Analysis (HRA) (Kirwan, 2017; Dimaio et al., 2021). Alternatively, there are some suggested rough PFD values for human actions and human barriers. For instance, the ARAMIS project provided the reference PFD values derived in an equivalent level of confidence (LC) for different types of human barriers, as shown in Table 1. Additionally, the quantification of the influence of the safety management system on QRA results through the audit of the safety management system quality/efficiency was suggested by both the ARAMIS project (Andersen et al., 2004) and the I-RISK project (Bellamy

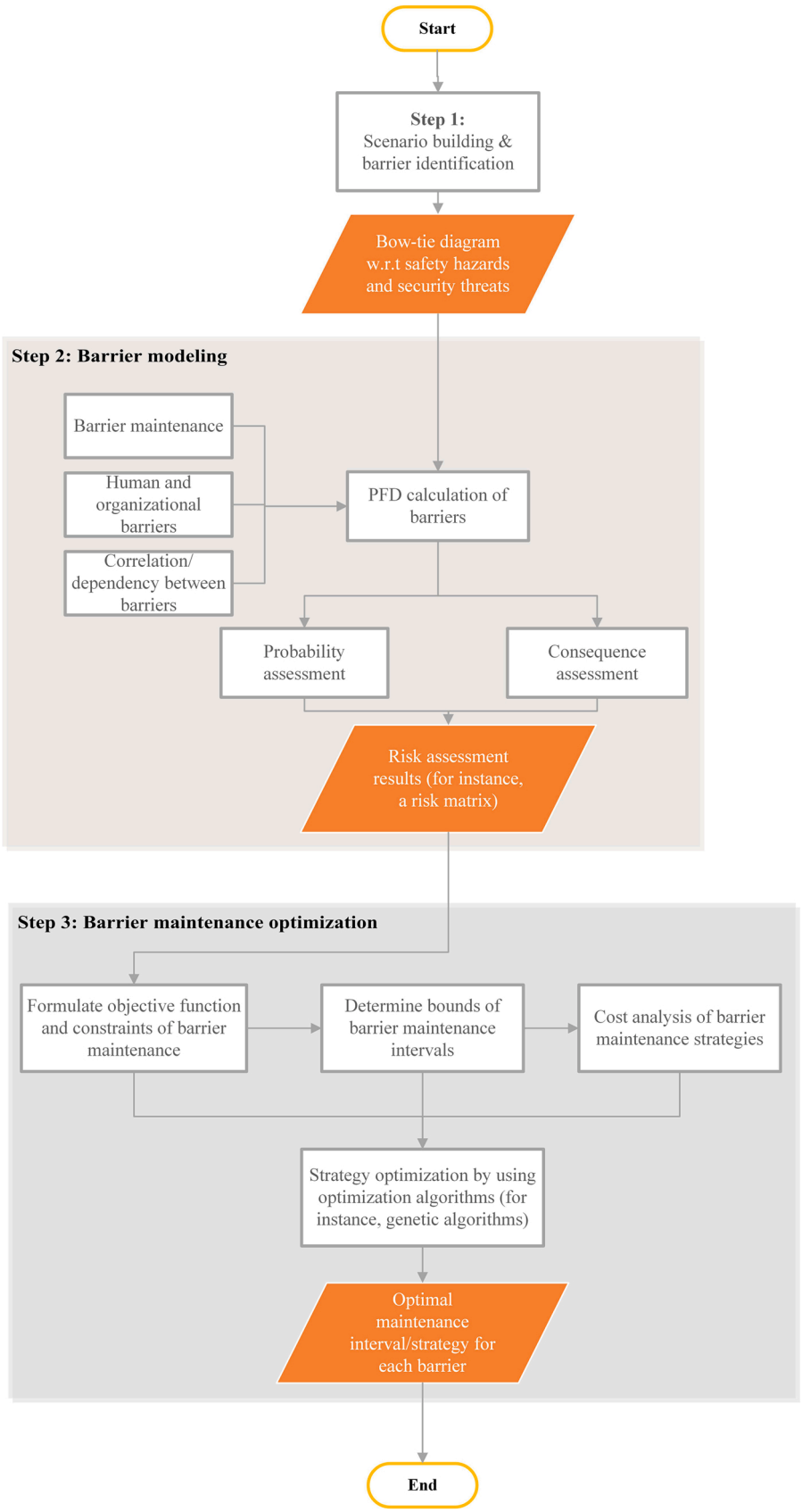

Fig. 1. The framework of the proposed approach.

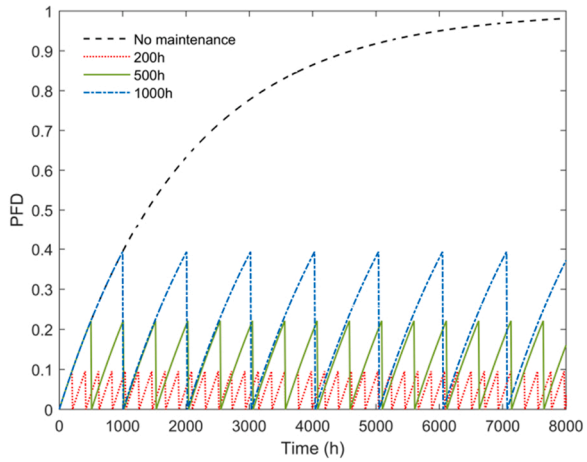

Fig. 2. The probability of failure on demand (PFD) of a barrier by using different maintenance intervals.

Table 1
Reference PFDs for human barriers, adapted from (Andersen et al., 2004).

Human barrier/human action types	PFD (from literature and industry)	Level of confidence
Prevention	10^{-2}	LC 2
Normal operation	10^{-2}	LC 2
Intervention	10^{-1}	LC 1

et al., 1999). The I-RISK project proposed a management model incorporating the organizational and management aspects that may affect the performance of people, and indirectly of the hardware (Papazoglou et al., 2003). ARAMIS project suggested evaluating the influence of safety management efficiency on safety barrier reliability by conducting site-specific questionnaires (Andersen et al., 2004).

2.3.3. Correlations between barriers

Based on the risk-based barrier maintenance/management concept, the performance of a barrier is measured by its effectiveness in risk reduction with respect to specific accident scenarios. For the barriers designed for reducing the risks of the same accident scenarios, their importance/criticality to risk reduction is correlated. In that case, the importance/criticality of one barrier in risk reduction is influenced by the reliability/availability of the other barriers because they have synergistic effects on risk reduction. Because both safety hazards and security threats can induce undesired accident scenarios, the assessment of safety and security barriers in a unified framework with the consideration of their synergistic effects on risk reduction is necessary. Therefore, an extended bow-tie model is used to identify accident scenarios in terms of both safety hazards and security threats (Section 2.2), and further, a dynamic barrier modeling approach is introduced to conduct a probabilistic risk assessment with the consideration of the synergistic effects of safety and security barriers on accident scenario risks.

Additionally, CCPS (USA) and the Energy Institute (UK) emphasized that active barriers should contain elements of 'detect-decide-act' and perform the complete intended function on its own when demanded (CCPS/EI, 2018). In real cases, it is possible that different barriers/-barrier systems have some commonly used components responsible for completing specific tasks. For instance, an automatic emergency shutdown system (ESD) and a manual shutdown (MS) may use the same detector for monitoring the abnormal parameters/events and perform the shutdown by using the same valve, as shown in Fig. 3. If we use independent PFDs for those barriers without consideration of their common components, the risk assessment results become wrong, and further, the reasonable/optimal barrier allocation and barrier maintenance strategy could not be obtained. For two safety barriers with a shared component and located on the same branch, a conditional probability $P_2^{'}$ instead of PFD should be used for the second barrier. The conditional probability can be calculated as follows (Duijm, 2009):

$$P_{1,R} = \frac{P_1 - P_C}{1 - P_C} \tag{5}$$

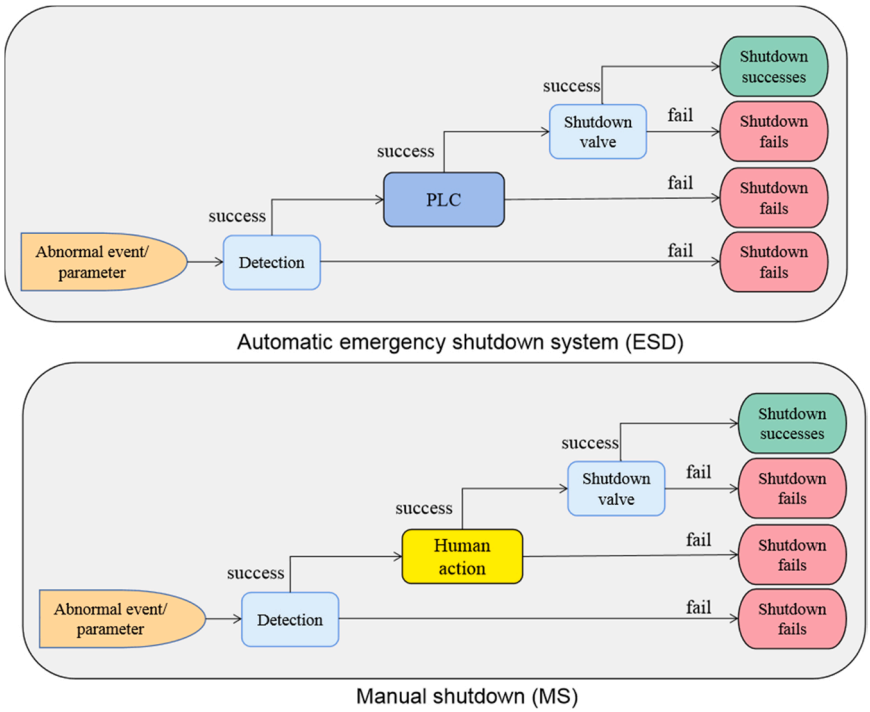

Fig. 3. A comparison between the components of an automatic emergency shutdown system (ESD) and manual shutdown (MS).

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

$$= P_{2,R} + P(C\ fails|B_1\ has\ failed)\left[1 - P_{2,R}\right] = P_{2,R} + (P_C/P_1)\left[1 - P_{2,R}\right] \quad (6)$$

where P_1 indicates the PFD of the barrier 1, which contains a common component C with a PFD P_C. $P_{1,R}$ is the PFD of the remaining components of the barrier 1 in series with component C. It should be notice that the above formulas can be adapted to calculate the conditional probabilities of multiple barriers with shared components as well, but those barriers have to situate on the same branch of the bow-tie (Duijm, 2009).

2.3.4. Probabilistic risk assessment

After the PFDs of barriers are determined, it is possible to conduct a probabilistic risk assessment of the undesired accident scenarios based on the bow-tie diagram obtained from step 1. As a combination of fault tree analysis and event tree analysis, bow-tie diagrams can perform probability calculations. By assigning the PFD values to the corresponding barriers and following the calculation rules of the bow-tie, a probability assessment can be conducted directly. Alternatively, bow-tie diagrams can be transformed into Bayesian network models for probability assessments (Khakzad et al., 2013).

Consequence assessment is an important part of risk assessment. There are many methods and tools available for quantitative and qualitative consequence assessment of major accident scenarios in the chemical process industries. For instance, some software (PHAST, ALOHA, Ansys Fluent, FLACS, etc.) based on empirical models or CFD models can be used for physical effects modeling (Lewis, 2005). The combination of CFD simulations and the probabilistic linear response model can be used for quantitative consequence assessment in terms of toxic leakage, fire, and explosion (Xie et al., 2022; Freeman, 1990). Other methods for quantitative consequence assessment were also suggested (Chen et al., 2021a; Van Den Bosh et al., 1989). Alternatively, qualitative consequence assessment is also applied widely in the chemical process industries. For instance, a class of consequences was proposed by the ARAMIS project, and the application of this class to typical dangerous phenomena was also presented, as shown in Table 2 and Table 3.

Table 2
Class of consequences, adapted from (Andersen et al., 2004).

Consequences			Class
Domino effect	Effect on human targets	Effect on environment	Ranking
To take into account domino effects, the class of consequence attributed to the studied dangerous phenomenon will be increased to the class of the secondary phenomenon that the first can bring about by domino effect	No injury or slight injury with no stoppage of work	No action is necessary; just watching	C_1
	Injury leading to a hospitalization > 24 h	Severe effects on the environment, requiring local means of intervention	C_2
	Irreversible injuries or death inside the site, Reversible injuries outside the site	Effects on environment outside the site, requiring national means	C_3
	Irreversible injuries or death outside the site	Irreversible effects on the environment outside the site, requiring national means	C_4

Table 3
Rough class of consequence of typical "fully developed" dangerous phenomena, adapted from (Andersen et al., 2004).

Dangerous phenomena	Consequence class
Pool fire	C_2
Tank fire	C_1
Jet fire	C_2
VCE	C_3 or C_4 (according to the released quantity)
Flash fire	C_3
Toxic cloud	C_3 or C_4 (according to the risk phrases – C_4 for very toxic substances)
Fire	C_2
Missiles ejection	C_3
Overpressure generation	C_3
Fireball	C_4
Environmental damage	To judge on site
Dust explosion	C_2 or C_3 (according to the substance and the quantity)
Boilover and resulting poolfire	C_3

2.4. Barrier maintenance optimization (step 3)

To make decisions on the implementation of protection systems or maintaining existing protection systems, which consist of a set of safety barriers and/or security barriers, an economic analysis is recommendable since the budget of a company for safety and security purposes is always limited (Chen and Reniers, 2021). This section illustrates the combination of cost-effectiveness analysis (CEA) and genetic algorithm (GA) for barrier maintenance optimization.

2.4.1. Cost-effectiveness analysis using constraints

The trade-off between safety and economy is a practical problem faced by chemical companies. For instance, the integration of safety-related aspects and economic aspects was highly emphasized in risk-based inspection (RBI) approaches (Jovanovic, 2003). There are also a couple of methods that are useful to address the trade-off between safety and economy (Reniers and Van Erp, 2016; Chen et al., 2021b). One of them is cost-effectiveness analysis (CEA), which has the advantages in conducting comparative studies and no need to monetize accident costs. The effectiveness of a strategy in CEA can be any safety indicator based on the preferences of decision-makers. In order to facilitate the integration of QRA and (CEA), the effectiveness of implementing a barrier maintenance strategy is measured by risk-associated indicators (e.g. risk reduction of specific accident scenarios after implementing this strategy). In this way, a comparison of the QRA results under implementing different strategies can be conducted to rank the effectiveness of those strategies.

Two typical practices for conducting CEA with constraints are i) a minimum acceptable level of effectiveness (Eff_{min}) and ii) a maximum acceptable use of safety budget (Bu_{max}). The first constraint applies to situations where a company has to reduce the risks of major accident scenarios below a certain level, corresponding to making the effectiveness of safety investment above a certain level (minimum effectiveness). The second constraint applies to a company that only has a limited budget (maximum budget) that can be used for safety investment. Those two constraints usually need to be matched with different objective functions. The optimization problems for imposing the two kinds of constraints w.r.t two alternative objective functions are as follows (Reniers and Van Erp, 2016):

$$\left\{ \begin{array}{c} Min(C_i) \\ Eff_i \geq Eff_{\min} \\ i \in \{1, 2, 3, \ldots, N\} \end{array} \right\} \quad (7)$$

or:

$$\left\{ \begin{array}{c} Max(Eff_i) \\ C_i \le Bu_{\max} \\ i \in \{1,2,3,\ldots,N\} \end{array} \right\} \quad (8)$$

where i means a strategy i from N possible strategies for the implementation and/or maintenance of safety and security barriers. C_i is the cost of the implementation of strategy i. Eff_i is the effectiveness (safety and/or security outcome) of the implementation of strategy i. The effectiveness (safety and/or security outcome) can be an indicator associated with safety and/or security according to the preferences of decision-makers (Chen et al., 2021b). In this study, the effectiveness of implementing a barrier maintenance strategy is measured by the corresponding risk reduction in terms of specific accident scenarios. It means that maximizing the effectiveness of barrier maintenance equals minimizing the risks of accident scenarios by using barrier maintenance.

2.4.2. Optimization algorithm

In terms of barrier maintenance optimization, a series of candidate strategies should be formulated at first. If only a limited number of candidate strategies can be formulated, the best strategy can be obtained through an exhaustive search. Otherwise, evolutionary algorithms (for instance genetic algorithms) help to solve the optimization problem with a large solution space. Because there are usually thousands or even millions of strategies in terms of barrier maintenance concerning the variations in maintenance interval of each barrier, the application of evolutionary algorithms becomes necessary. For instance, the maintenance interval of a barrier can vary from the shortest time step (1 h in this study) to the maximum maintenance interval defined by users according to company regulations or referencing to related standards. In that case, it becomes unreasonable to assess all the maintenance strategies by an exhaustive method. By contrast, evolutionary algorithms have the potential to solve this optimization problem by determining the optimal barrier maintenance strategy under economic constraints or technical constraints. Genetic algorithms (GA) have proven to be able to solve multivariable, nonlinear, and combinatorial optimization problems where the solution space can be huge and too vast to search exhaustively in a reasonable amount of time (Caputo et al., 2011). Generally, GAs have five steps: i) initial population, ii) fitness function, iii) selection, iv) crossover, and v) mutation. After population initialization, the genetic algorithm selects individuals from the current population to be parents and uses them to produce the children for the next generation at each step. There are mainly three kinds of rules for creating the next generation from the current population. They are i) selection rules generally randomly select the individuals as parents that contribute to the next population generation; ii) crossover rules combine two parents to form children for the next generation; and iii) mutation rules apply random changes to individual parents to form children. A detailed illustration of GA can be found in Goldberg (1989) and Caputo et al. (2011).

In terms of the safety optimization problem, the GA minimizes the objective function with respect to all the constraints and determines the optimal strategy within the entire space of possible solutions. The procedures of employing GA for solving the above-mentioned two kinds of CEA optimization problems (formula 7 and formula 8) are shown in Fig. 4. This study uses a genetic algorithm toolbox based on MATLAB to solve barrier maintenance optimization problems.

3. A system simulation tool for barrier modeling

To facilitate the implementation of the proposed approach in practice, a system simulation approach based on the MATLAB Simulink platform (Chaturvedi, 2017) is developed to conduct dynamic barrier modeling. The Simulink-based dynamic barrier modeling can be developed based on the obtained bow-tie diagram from step 1 (presented in Section 2.2). Then, the dynamic barrier modeling is employed to conduct the probabilistic risk assessment with the consideration of

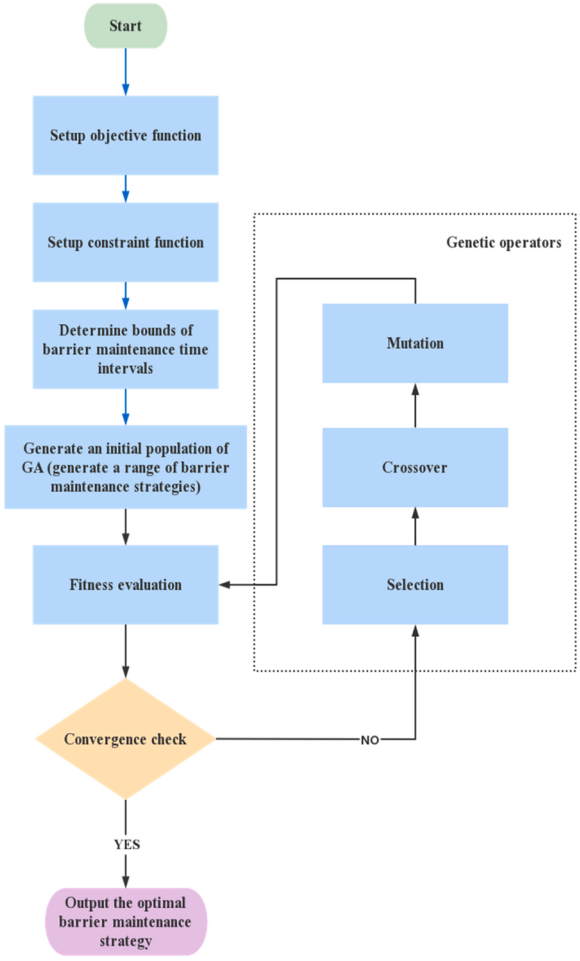

Fig. 4. Genetic algorithm developed for safety and security barrier maintenance optimization.

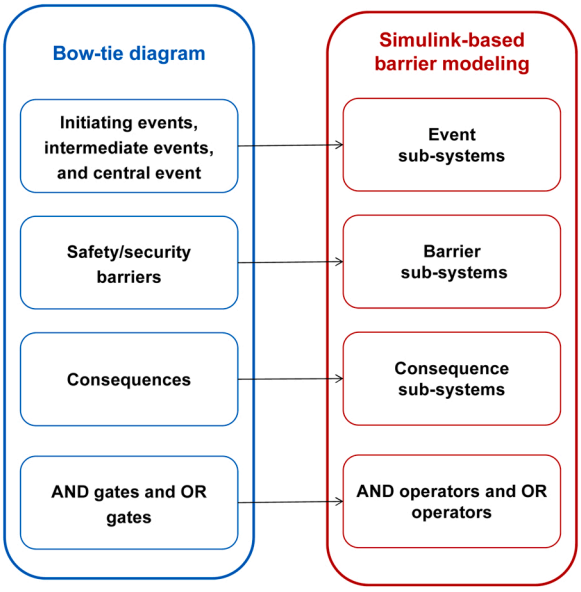

Fig. 5. Flowchart of mapping algorithm from bow-tie to Simulink-based barrier modeling.

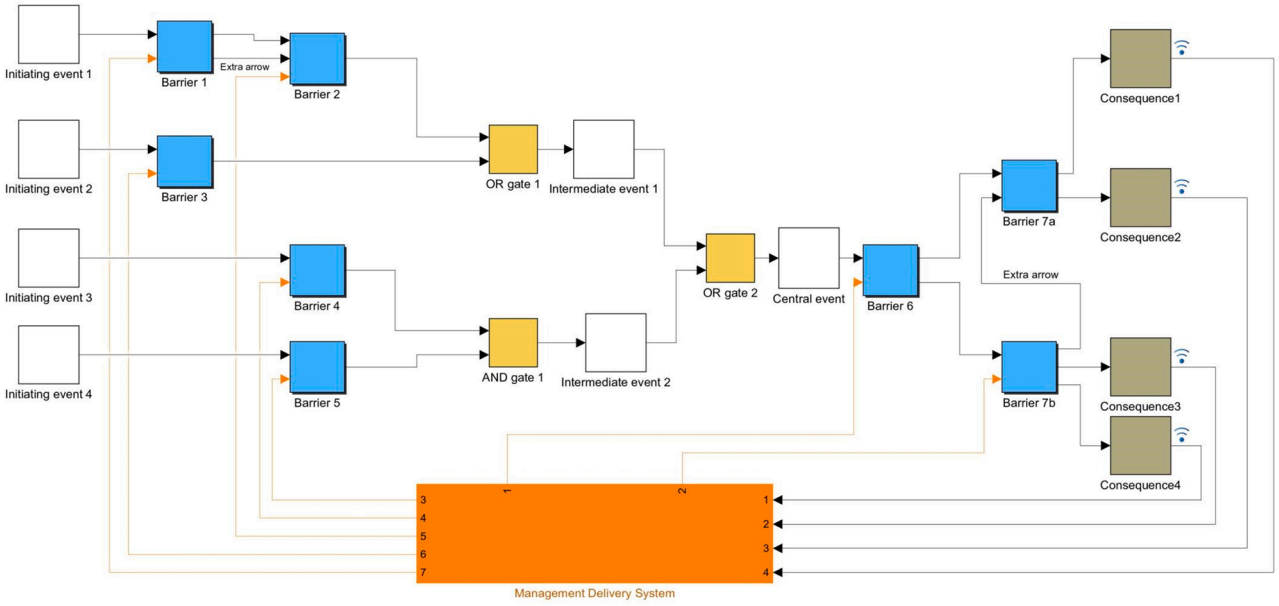

Fig. 6. Barrier modeling based on Simulink simulation.

time-varied PFDs of barriers. The inputs for the dynamic barrier modeling are failure data of the barrier components and occurrence probabilities of the initiating events. The output of the simulation is a risk matrix with respect to major accident scenarios/dangerous phenomena (VCE, flashfire, toxic cloud, etc.). A mapping algorithm for converting a bow-tie diagram into a Simulink-based barrier model is given in Fig. 5. By following this mapping algorithm, the obtained accident scenarios presented by a bow-tie diagram can be transformed into a system simulation model, as shown in Fig. 6. All events, barriers, and consequences in the bow-tie diagram become sub-systems in the barrier modeling approach. "Event" sub-systems contain the frequencies or probabilities of such events happening. "Consequence" sub-systems contain information associated with both the frequencies/probabilities and the severities of such consequences. In this study, the consequence assessment method proposed by the ARAMIS project is used and incorporated into the "consequence" sub-systems. "Barrier" sub-systems aim to calculate the time-dependent PFDs of such barriers. Instead of transporting physical parameters between sub-systems, the arrows in the barrier model mainly transport probabilities, thus achieving a quantitative probability assessment. The basic rules for the probability calculation are adapted from the fault tree (Haasl et al., 1981) and event tree (Andrews and Dunnett, 2000), including the logical operators: AND gate and OR gate. PFDs of barriers can be calculated or determined according to the methods illustrated in Section 2.3.1 to Section 2.3.3. The fault tree analysis of barriers can also be performed based on the Simulink simulation platform. The fault tree analysis can be incorporated into the "barrier" sub-system, which integrates fault tree analysis and dynamic bow-tie modeling together to achieve a unified simulation. For instance, for a barrier with the elements/functionalities of 'detect--decide-act', the different functionalities are achieved by using different components. The PFD of this barrier can be calculated by using a fault trees analysis, which is performed inside the "barrier" sub-system, as

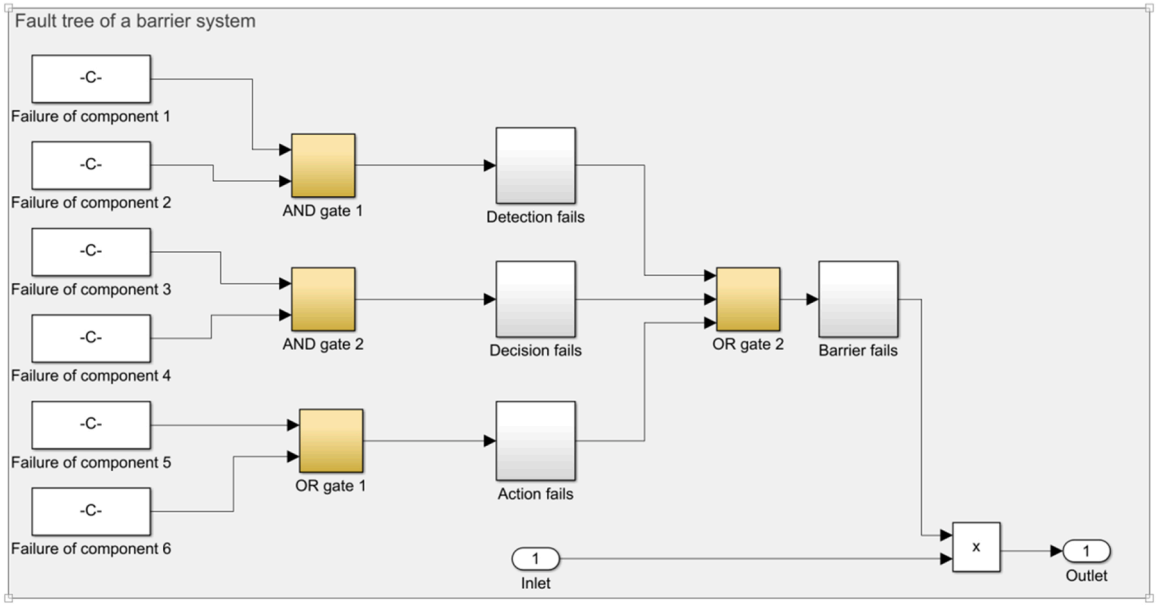

Fig. 7. Fault tree of a barrier system performed inside the "barrier" sub-system.

shown in Fig. 7. If different barriers use some shared components, extra arrows should be used to link such barriers and transport necessary parameters (PFDs in this study) of the shared components to ensure the correlation among barriers is considered in the barrier PFD calculation (as mentioned in Section 2.3.3). It is also possible that a barrier can be placed on multiple branches on the right-hand side of a bow-tie because this barrier can be used in different scenarios (for example, Barrier 7a and Barrier 7b in Fig. 6 demonstrate the same barrier, and are located on different branches). In that case, extra arrows should link those barriers that indicate the same barrier and transport time-dependent PFD values to ensure consistent PFDs are used. We marked the extra arrows in Fig. 6.

Our previous study defined management delivery systems (MDS) as a set of organizational and management factors that can prevent or mitigate undesired events indirectly and mainly play a role by enhancing/maintaining the performances of the scenario-specific barriers or increasing the accident response capabilities of the overall system (Yuan et al., 2022c). By using the concept of MDS, the barrier-associated organizational and management factors can be involved in the barrier modeling. In this study, a sub-system named "management delivery system" is used in the barrier modeling to tackle several tasks: i) collect risk assessment results, including both the probabilities/frequencies and severities of the consequences, ii) determine time intervals for barrier maintenance and give instructions to barrier sub-systems, iii) evaluate organizational and management factors associated with barriers and determine PFDs for human barriers or human components of barriers. As shown in Fig. 6, the arrows with orange color are used to transport parameters from MDS to barriers. Additionally, due to the flexibility and compatibility of the MATLAB/Simulink simulations, various optimization algorithms (exhaustive search algorithms, evolutionary algorithms, etc.) can be integrated with the Simulink-based barrier modeling for cost-effective barrier maintenance optimization. For instance, a genetic algorithm toolbox is available for solving the optimization problem with a large solution space (Mathworks, 2022).

4. Case study

In this section, an illustrative case is conducted to validate the feasibility of the proposed approach. This case study is elaborated in three parts: scenario building, barrier modeling, and barrier maintenance optimization. In this case, for illustrative purposes, only one accident scenario of a reactor wall rupture leading to leakage, is demonstrated.

4.1. Scenario building

A typical chemical reactor with its SCADA (supervisory control and data acquisition) system is investigated in this case study. The basic process control system of this reactor is adapted from Abdo et al. (2018), while an ESD system is considered as a system independent of the basic process control system, as shown in Fig. 8. This reactor is used to run a chemical reaction in order to produce product C from two reactants A and B. We assumed that this reactor is used to produce a flammable liquid with toxicity, for instance, propylene oxide. The ESD system controls the block/shutdown valves (XV33012 and XV33013) in case of over-pressure based on the monitored pressure inside the reactor. The basic process control system includes a feeding system and a cooling system, which are controlled by PLC1 and PLC2, respectively. The temperature of the reaction is regulated with industrial water, and the temperatures of the water inside the cooling jacket and at the inlet are measured by the sensor TI and T2, respectively. The data collected by these two sensors is sent to PLC2, which regulates the water flow rate by controlling pumps (P1 and P2, P2 is a standby pump) and valves (CV33063 and XYSV33027). The physical components (valves, pumps, etc.) of the basic process control system are controlled by PLCs and supervised by a SCADA system. Site managers can access the information collected by the SCADA system and control the reaction process remotely inside the control center.

According to the structure of this process control system, the

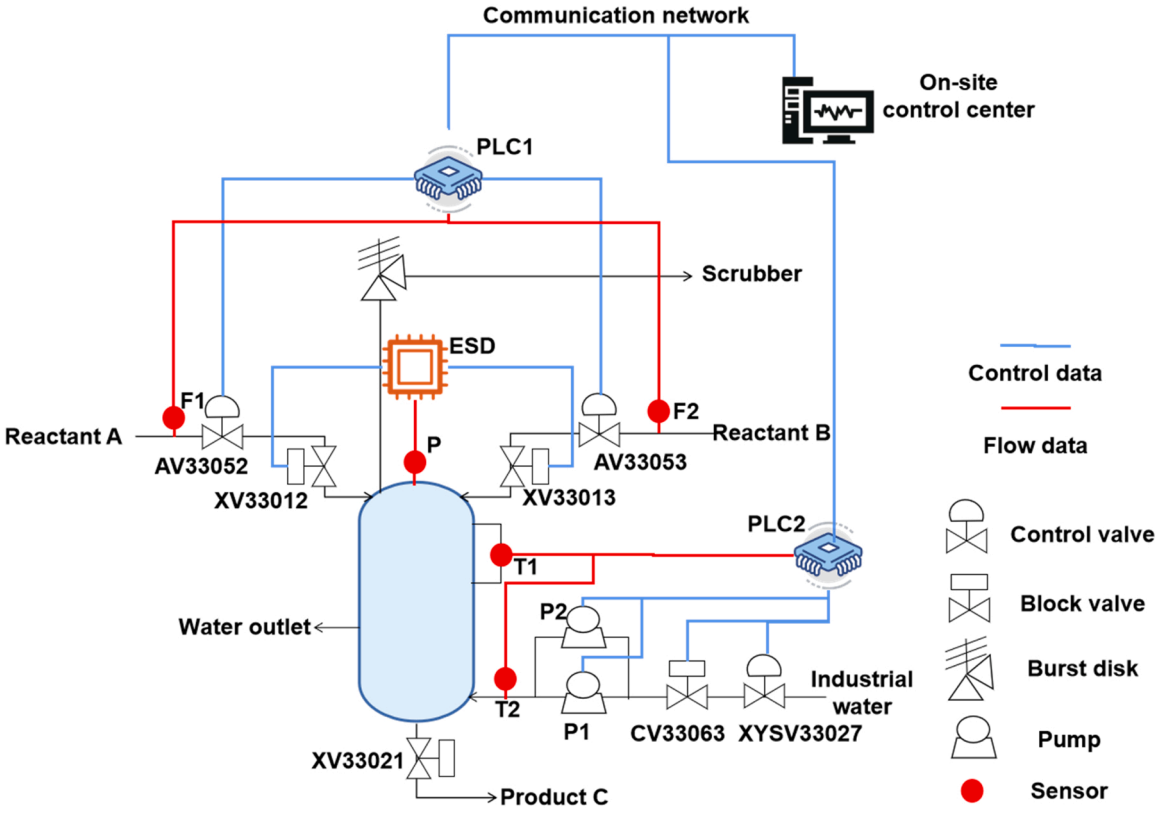

Fig. 8. The investigated chemical reactor with its SCADA system, adapted from (Abdo et al., 2018).

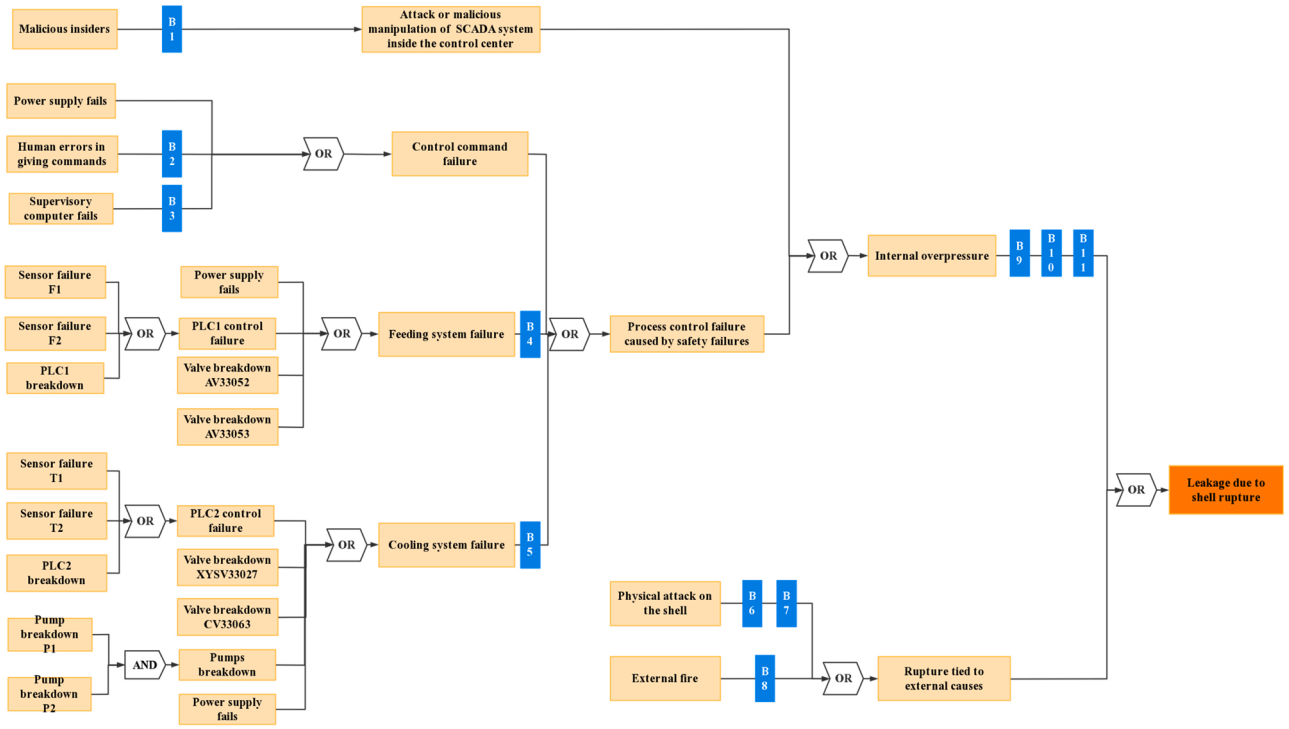

Fig. 9. Fault tree of the chemical reactor with propylene oxide leakage as the top event.

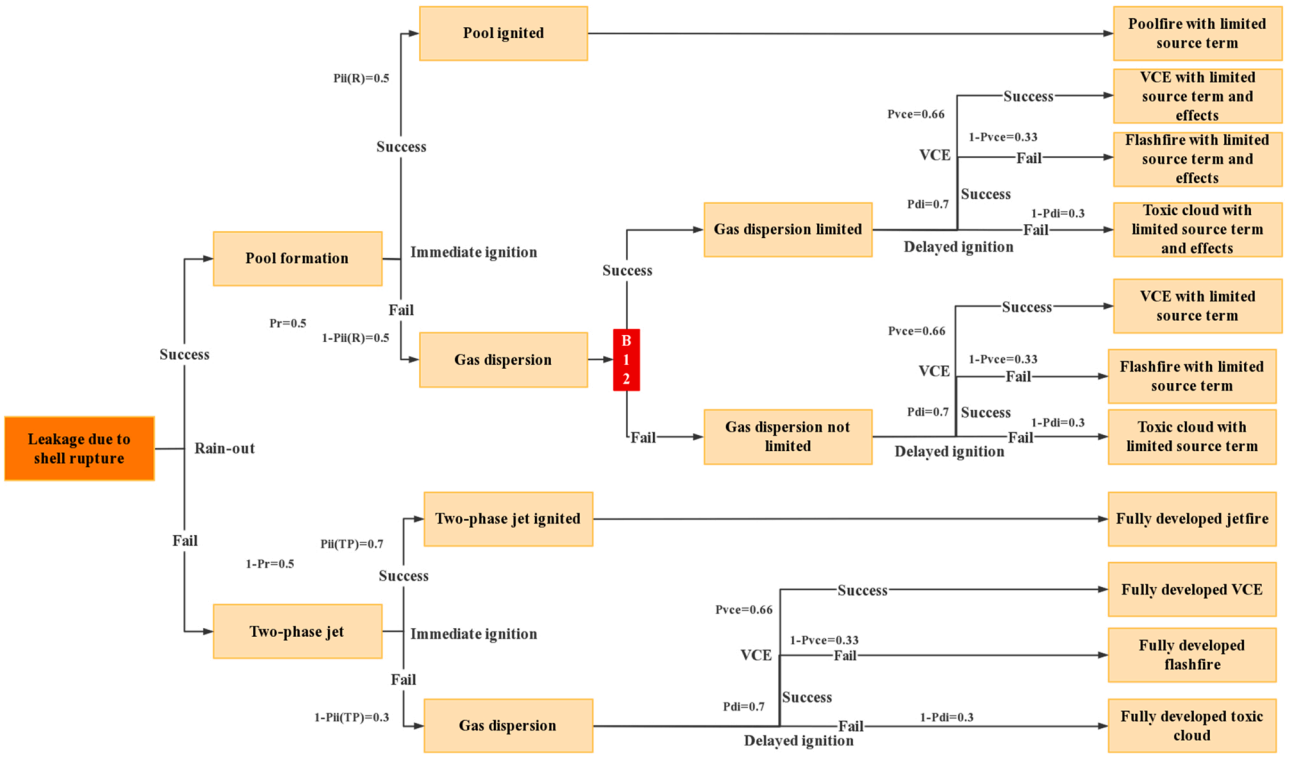

Fig. 10. Event tree of the chemical reactor with propylene oxide leakage as the initiating event, adapted from (Andersen et al., 2004).

propylene oxide leakage scenarios in terms of safety failures and malicious acts can be built by using a bow-tie diagram, which consists of a fault tree and an event tree, as shown in Fig. 9 and Fig. 10 respectively. Associated safety and security barriers were identified and allocated on the bow-tie diagram according to the database/checklists from (Andersen et al., 2004), (Argenti et al., 2017), and (Guzman et al., 2021). The explanations of the barriers in Fig. 9 and Fig. 10 are given in Table 4.

4.2. *Barrier modeling configurations and results*

This study aims to provide a system simulation approach for

Table 4
Explanations of barriers in the bow-tie diagram (Fig. 8 and Fig. 9).

Marks	Barriers	Marks	Barriers
B1	Entrance control system (unsupervised automatic credentials check)	B2	Training and authorization before work
B3	Inspection of supervisory computers	B4	Inspection of feeding system
B5	Inspection of cooling system	B6	Entrance control (unsupervised automatic biometrics check)
B7	Guard response	B8	Fire protection system
B9	Emergency shutdown system (ESD)	B10	Manual shutdown (MD)
B11	Burst disk	B12	Foam injection

Table 5
Frequencies of basic events in the barrier modeling.

Events	Frequencies (y^{-1})	Events	Frequencies (y^{-1})
Malicious insiders	3.3E− 02 (Landucci et al., 2017)	Physical attack	3.3E− 02 (Landucci et al., 2017)
Power supply fails	1.00E-01 (Çetinkaya, 2001)	Human error in giving commands	1.00E-02 (Andersen et al., 2004)
Supervisory computer fails	5.00E-04 (Çetinkaya, 2001)	PLC1 breakdown	4.38E-02 (Hauge and Onshus, 2010)
Sensor failure F1	3.50E-01 (Debray et al., 2004)	Sensor failure F2	3.50E− 01 (Debray et al., 2004)
Valve breakdown AV33052	4.00E-02 (Taylor, 2010)	Valve breakdown AV33053	4.00E-02 (Taylor, 2010)
PLC2 breakdown	4.38E-02 (Hauge and Onshus, 2010)	Pump breakdown P1	3.125E-02 (OREDA, 2002)
Pump breakdown P2	3.125E-02 (OREDA, 2002)	Valve breakdown XYSV33027	4.00E-02 (Taylor, 2010)
Valve breakdown CV33063	4.00E-02 (Taylor, 2010)	Sensor failure T1	2.13E-02 (Hauge and Onshus, 2010)
Sensor failure T2	2.13E-02 (Hauge and Onshus, 2010)	External fire	5.52E-02 (Debray et al., 2004)

conducting risk assessments of chemical process control systems based on the MATLAB/Simulink platform. Frequencies of the basic events in Fig. 8 are retrieved from other studies or datasets and are given in Table 5. The frequency of adversary attacks is adapted from (Landucci et al., 2017), in which the annual attack probability for chemical facilities in Italy was investigated. Configurations of the associated safety and security barriers and barrier components, including their failure rates/PFDs, maintenance time, and initial maintenance intervals, are given in Table 6. For simplification purposes, the maintenance times of all technical barrier components are set as 8 h. In practice, the barrier maintenance time can be configured according to the practical experience of workers. The initial maintenance interval for a technical barrier component is set as 500 h. Constant PFDs are used to describe the performance of security barriers and human barriers/human actions in this case study due to the lack of historical data and the difficulties in formulating the time-varied PFDs for such barriers. Failure probabilities of the security barriers are mainly retrieved from (Argenti et al., 2017). As a result, the maintenance of all technical safety barriers or technical components of safety barriers is considered in the barrier modeling. With more data and studies on the evaluation of the time-dependent performance/PFDs of security barriers becoming available, the integrated optimization of safety and security barrier maintenance can also be achieved by employing the proposed methodology.

The developed barrier model with respect to hazardous scenarios caused by safety failures and malicious acts/physical attacks is shown in Fig. 11. In order to simplify the barrier modeling, the basic events for calculating feeding system failure frequency and cooling system failure frequency are not presented in the barrier model. The frequencies of feeding system failure and cooling system failure should still be calculated according to the fault tree by using the frequencies of their associated basic events. Using this barrier modeling, a dynamic probability/frequency assessment can be performed. With the combination of the consequences class proposed by the ARAMIS project and the calculated yearly-average frequency of each consequence in the barrier modeling, the frequency and severity of each consequence can be presented in a risk matrix, as shown in Fig. 12. A list of the consequences in the risk matrix is shown in Table 7.

As shown in Fig. 12, the major consequences of the accidental scenarios are the dots with numbers 1, 5, and 10, corresponding to “fully developed VCE”, “VCE with limited source term”, and “VCE with limited source term and effects”. Since those consequences are in the red region, which means they correspond to unacceptable risks, barrier maintenance improvement should be conducted to ensure that the probabilities of all consequences become situated in the yellow region (acceptable with mitigation) or green region (acceptable). The next section elaborates on how to achieve this optimization by employing the proposed GA-based method.

4.3. Barrier maintenance optimization

A genetic algorithm (GA) is employed in this study to solve the trade-off problem between the cost of barrier maintenance and the potential risks associated with flammable liquid leakage of chemical reactors. The cost analysis of barrier maintenance and the GA-based optimization of barrier maintenance intervals are presented in the below sub-sections.

4.3.1. Cost analysis of barrier maintenance

In order to optimize the existing barrier maintenance strategy, a cost analysis of a series of candidate strategies should be conducted. Then, it is possible to determine the most cost-effective strategy through cost-effectiveness analysis (CEA). Usually, cost analysis for a protection measure (safety or security barrier) should include the direct economic costs of applying the measure and indirect costs associated with its use (Chen et al., 2021b). Reniers and Van Erp (2016) illustrated eight cost categories of protection measures for safety barriers, and the maintenance cost includes the costs for material, maintenance team, production loss, and start-up. Due to the difficulties in obtaining all the costs for barrier maintenance, we assumed that the one-time costs for material consumption and maintenance team of the technical barrier maintenance are 10~50 % of the purchase price of the products (for small technical components, the cost of maintenance team may take the main part). In some situations, the maintenance of safety barriers (mainly preventive barriers) has to break off the production process (Wu et al., 2022). In that case, a downtime cost should be considered. We assumed that the downtime cost per hour is 10 thousand € and the downtime cost only applied to the ESD system in this case study. We list the maintenance costs (exclude downtime costs) for all the technical barrier components in Table 6. In practice, those costs should be configured according to the real expenses of the companies.

4.3.2. GA-based barrier maintenance strategy optimization

According to the obtained risk matrix, the risks of “fully developed VCE”, “VCE with limited source term”, and “VCE with limited source term and effects” are not acceptable. Therefore, the optimization objective is to minimize barrier maintenance costs with the constraints that ensure all consequences are at least in the yellow region in the risk matrix. The objective function to be minimized is:

$$C = \sum_{i=1}^{n} U_i * N_i \tag{9}$$

where C is the annual total cost of barrier maintenance that can be

Table 6
Configurations of safety and security barriers.

Number	Barriers	Barrier components	Failure rates (/h)	PFDs	Maintenance time (h)	Initial maintenance intervals (h)	One-time maintenance cost (exclude downtime cost) (€)
1	Entrance control system (unsupervised automatic credentials check)	/	/	1.0E-02 (Argenti et al., 2017)	/	/	/
2	Training and authorization before work	/	/	1.0E-02 (Andersen et al., 2004)	/	/	/
3	Inspection of supervisory computers	/	/	1.0E-01 (Andersen et al., 2004)	/	/	/
4	Inspection of feeding system	/	/	1.0E-01 (Andersen et al., 2004)	/	/	/
5	Inspection of cooling system	/	/	1.0E-01 (Andersen et al., 2004)	/	/	/
6	Entrance control (unsupervised automatic biometrics check)	/	/	1.0E-02 (Argenti et al., 2017)	/	/	/
7	Guard response	Alarm assessment through CCTV system	/	3.0E-02 (Argenti et al., 2017)	/	/	/
		Communication to response force	/	5.0E-02 (Argenti et al., 2017)			
		Guard force response	/	1.62E-02 (Song et al., 2019b)			
8	Fire protection system	Smoke/combustion detector	4.12E-06 (OREDA, 2002)	/	8	500	150 €
		Programmable logic solver	1.0E-06 (Hauge and Onshus, 2010)	/	8	500	300 €
		Fire pump	7.2E-5 (Gravestock, 2008)	/	8	500	300 €
		Deluge Valve	5.8E-06 (Gravestock, 2008)	/	8	500	200 €
9	Emergency shutdown system (ESD)	Pressure sensor[a]*	1.5E-07 (Hauge and Onshus, 2010)	/	8	500	150 €
		Programmable safety system	1.0E-06 (Hauge and Onshus, 2010)	/	8	500	300 €
		Shutdown valve XV33012*	3.5E-06 (Hauge and Onshus, 2010)	/	8	500	200 €
		Shutdown valve XV33013*	3.5E-06 (Hauge and Onshus, 2010)	/	8	500	200 €
10	Manual shutdown (MD)	Pressure sensor*	1.5E-07 (Hauge and Onshus, 2010)	/	8	500	150 €
		Human action	/	1.0E-02 (Andersen et al., 2004)	/	/	/
		ESD Push Button	1.2E-06 (Hauge and Onshus, 2010)	/	8	500	100 €
		Shutdown valve XV33012*	3.5E-06 (Hauge and Onshus, 2010)	/	8	500	200 €
		Shutdown valve XV33013*	3.5E-06 (Hauge and Onshus, 2010)	/	8	500	200 €
11	Burst disk	/	2.3E-05 (Lees, 1980)	/	8	500	200 €
12	Foam injection	Human response/ intervention	/	1.0E-01 (Andersen et al., 2004)	/	/	/
		Injection pump	2.31E-06 (OREDA, 2002)	/	8	500	300 €
		Injection valve	1.862E-05 (OREDA, 2002)	/	8	500	200 €

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

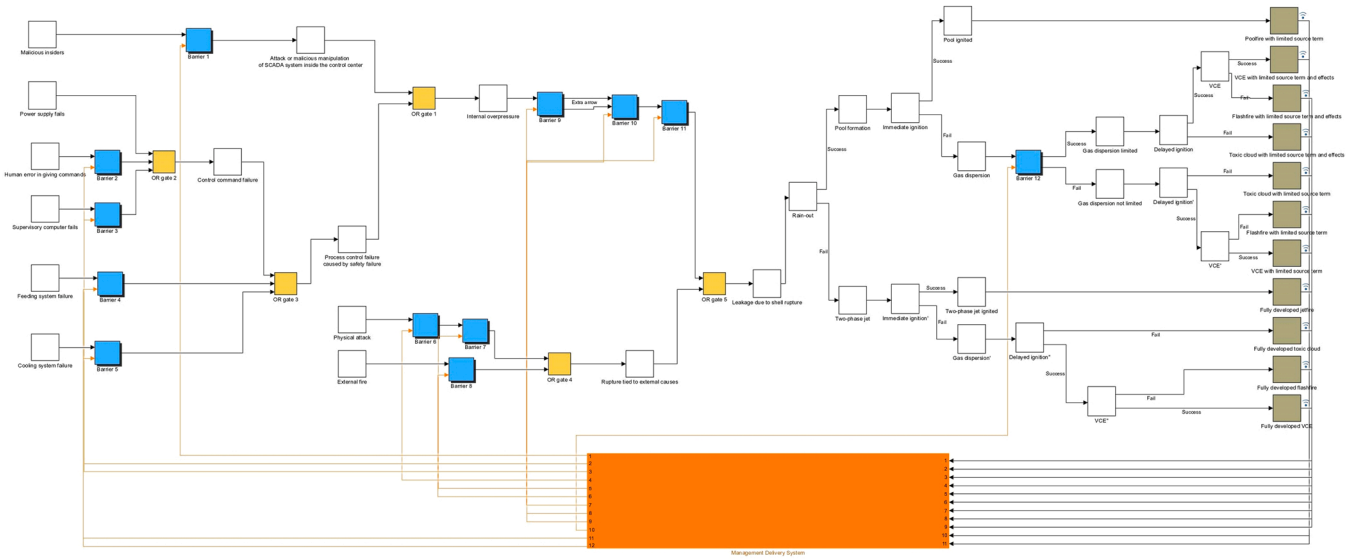

Fig. 11. Barrier modeling with respect to flammable liquid leakage scenarios caused by chemical reactor shell rupture.

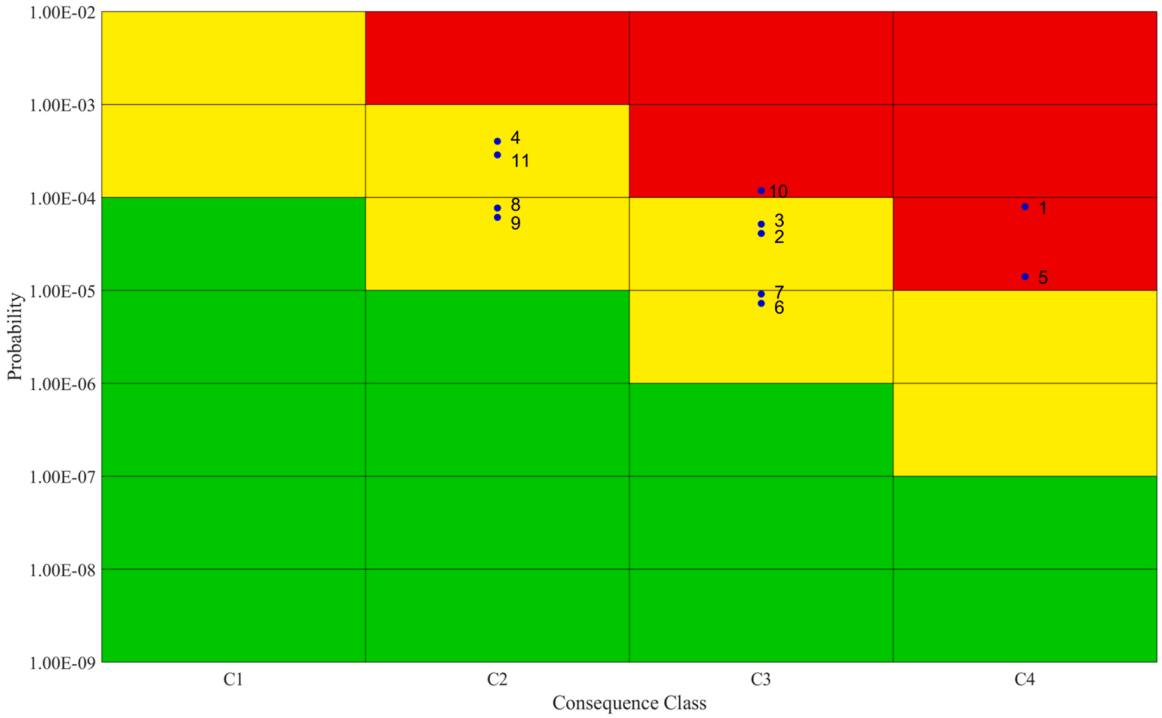

Fig. 12. Risk matrix of accidental scenarios (consequence class is configured according to Table 2; Note: numbers represent the consequence numbers, the corresponding consequence names can be found in Table 7).

calculated by summing the maintenance cost for each barrier. n is the number of barriers that need to be maintained. U_i is the unit price for maintenance of barrier i and N_i is the number of maintenance of barrier i in one year. The nonlinear inequality constraint is:

$$\left\{ \begin{array}{c} P_j \le TS_j \\ \\ j \in \{1,2,3,\ldots,N\} \end{array} \right\} \tag{10}$$

where P_j is the probability of consequence j. TS_j is the threshold for consequence j. N is the number of consequences in the risk matrix. The thresholds were set according to the boundaries of the yellow region in the risk matrix. Bounds of the barrier maintenance intervals were set as 1 h ~ 500 h. An integer constraint was applied to barrier maintenance intervals, which means that the barrier maintenance intervals have to be integers. A genetic algorithm toolbox based on MATLAB R2022a was used to solve this optimization problem. This toolbox is capable to solve smooth and non-smooth optimization problems with different types of constraints, including integer constraints. It searches the optimal strategy randomly by mutation and crossover among a large number of population members. More instructions on how to use this toolbox can be found in (Mathworks, 2022). The calculation results of the genetic algorithm are shown in Fig. 13. It can be observed that the individual penalty values (annual costs of barrier maintenance of individual strategies) are distributed approximately randomly within a relatively small region after a few generations of genetic evolution. The best penalty

Table 7
Table of consequences in the risk matrix.

Number	Consequence	Class	Number	Consequence	Class
1	Fully developed VCE	C_4	2	Fully developed flashfire	C_3
3	Fully developed toxic cloud	C_3	4	Fully developed jetfire	C_2
5	VCE with limited source term	C_4	6	Flashfire with limited source term	C_3
7	Toxic cloud with limited source term	C_3	8	Toxic cloud with limited source term and effects	C_2
9	Flashfire with limited source term and effects	C_2	10	VCE with limited source term and effects	C_3
11	Poolfire with limited source term	C_2	/	/	/

value (minimal annual cost of barrier maintenance) is 1,479,150 € after more than 250 generations of genetic evolution, which indicates the annual total cost of barrier maintenance is 1,479,150 € by using the optimal strategy obtained by the genetic algorithm. Meanwhile, the mean penalty value at the end is 6,572,570 €, which is the average cost of all individual barrier maintenance strategies. The corresponding optimal strategy for barrier maintenance is presented in Table 8, in which the optimal maintenance interval for each barrier/barrier component is provided.

5. Discussion

5.1. Benefits of GA-based barrier maintenance optimization

In this study, a case study was used to validate the feasibility of combining GA and CEA for tackling barrier maintenance optimization with respect to both safety failures and security attacks. In practice, barrier maintenance optimization is a nonlinear optimization problem involving multivariable that is unrealistic and unreasonable to search all strategies exhaustively. By implementing GA, the barrier maintenance optimization problems under economic constraints and technical constraints can be solved within affordable computation times. Additionally, the proposed approach has broad applicability due to the flexibility of GA. Users can easily add constraints or change the optimization objective by modifying the constraint functions or objective functions. Compared with directly reducing the maintenance intervals of all barriers to achieve acceptable risk levels, implementing the proposed approach can achieve the same goal at a lower cost. Such as, in the case study provided in Section 4, by reducing the maintenance interval of all barriers to 45 h, the risks of possible consequences are all at acceptable levels, and the annual cost of barrier maintenance is 13.63 M€ (including downtime cost). By contrast, the yearly cost of barrier maintenance is 1.48 M€ (including downtime cost), considering ensuring the risks of all possible consequences are at acceptable levels by using the proposed GA-based barrier maintenance optimization. It means that a large amount of the barrier maintenance cost can be saved by using the proposed approach.

5.2. Advantages of the proposed approach and recommendations for future work

The proposed approach combines QRA and CEA for barrier maintenance optimization with the consideration of risk sources including both safety hazards and malicious acts. Dynamic barrier modeling is conducted based on the MATLAB/Simulink platform to perform probabilistic risk assessment, and GA is employed to determine the optimal maintenance interval for each barrier. Compared to previous maintenance optimization approaches (such as RCM and RBI), the proposed approach has the advantage of integrating safety and security scenarios together for risk analysis and further optimizing the barrier maintenance strategy based on the synergistic effects of barriers on system risk reduction, rather than evaluating each barrier according to its own

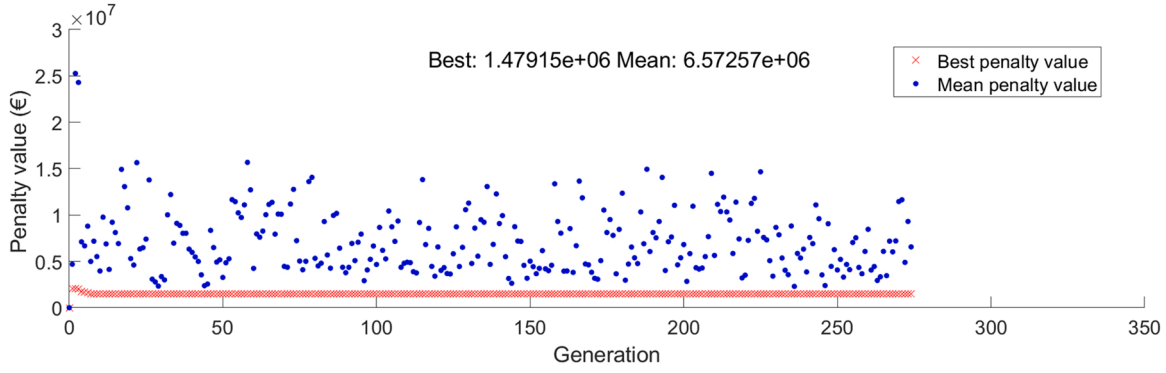

Fig. 13. Calculation results of the genetic algorithm.

Table 8
Optimal strategy for barrier maintenance.

Barriers	Technical components	Maintenance intervals (h)	Barriers	Technical components	Maintenance intervals (h)
Fire protection system	Smoke/combustion detector	137	Emergency shutdown system (ESD)	Pressure sensor	489
	Programmable logic solver	411		Logic solver	
	Fire pump	33		Shutdown valve XV33012	
	Deluge Valve	135		Shutdown valve XV33013	
Manual shutdown (MD)	ESD Push Button	479	Foam injection	Injection pump	485
				Injection valve	485
Burst disk	/	489	/	/	/

probability of failure and consequence of failure. Another advantage of the proposed approach is that the implementation of GA addresses the large solution optimization problems well, the optimal barrier maintenance strategy considering the specific maintenance interval of each barrier can be obtained by using this approach. Simulink as one toolbox of MATLAB is widely used in process control and dynamics modeling. The proposed approach provides a way to use a toolbox that is familiar to academics and professionals in chemical process industries for safety barrier modeling and then optimizing the barrier maintenance from a cost-effective perspective. That is another contribution of this study.

Although an illustrative case study was employed to validate the feasibility of the proposed approach, several improvements with respect to applying this approach in practice should be addressed in future works. They are listed hereafter.

i) In the proposed approach, barrier maintenance strategy is optimized based on the probabilistic risk assessment results, which also means uncertainty is inevitable involved in the approach. Uncertainties in a risk assessment usually subject to the occurrences of the undesired event and its consequences, the assumptions made based on background knowledge may hide or camouflage the uncertainties. Selvik and Aven (2011) emphasized the importance of the identification and assessment of the uncertainty factors associated with the assumptions made in the reliability centered maintenance (RCM). Similarly, we identify the uncertainty factors in the proposed approach hereafter, a uncertainty analysis may be performed in future studies or when apply the proposed approach in practice. The identified uncertainty factors include:
    - Failure data derived from readability databases were used for technical barrier components. The representativeness of the failure data brings uncertainties to the barrier maintenance optimization results.
    - Cumulative probabilities based on constant failure rates were used for PFD calculation of barriers. Although random failures dominate the failure distribution of many equipment units, the uncertainty caused by this simplification may be unacceptable in some practical applications.
    - Rough suggested values for human error probabilities were used.
    - Perfect maintenance is assumed, which means the performance of a barrier is assumed can restore to its original state after the barrier maintenance. But in practice, it may not always be like that.
    - The failure probability of a technical component is assumed following a linear descending distribution during the maintenance period.
    - The rationality of the risk threshold selected for barrier maintenance optimization is also an uncertainty factor. Due to those uncertainty factors, the obtained optimal strategy does not mean perfectly safe with saving costs. The alleviation of uncertainties and also the treatment and assessment of uncertainties in the barrier maintenance optimization may be focused on in future works.

ii) In this paper, exponential distributions were used to describe the time-varied PFDs of safety barriers. This is a relatively rough assumption and can be replaced by some more advanced models. For instance, the model with the consideration of multi-state transition of safety barriers (Wu et al., 2022), the model considering barrier degradation caused by aging degradation and damage caused by shocks (Pishro-Nik, 2016), and the model considering a series of intermediate factor (operation time, temperature, wind speed, pressure, and humidity) (Ouache et al., 2015). The integration of more sophisticated models for describing barrier degradation into the proposed approach helps to improve the accuracy of the results.

iii) Finally, due to the lack of data related to security barriers, evaluating such barriers is challenging, and thus, the maintenance of such barriers is not considered in this study. With more data related to the performance of security barriers available, the quantitative assessment and maintenance/allocation optimization of security barriers will also be possible by employing the proposed approach.

6. Conclusions

This study investigates possible optimal barrier maintenance intervals concerning both safety hazards and security threats in chemical plants from the cost-effectiveness perspective. The results show that the combination of bow-tie diagram and Simulink-based simulation for barrier modeling is effective for risk assessment of accident scenarios considering the synergistic effects of barriers on risk reduction. Based on barrier modeling results, cost-effectiveness analysis and a genetic algorithm can be combined to determine the optimal barrier maintenance strategy under economic constraints. Using the proposed approach for maintenance interval optimization of safety and security barriers makes it possible to obtain acceptable risk levels with much less cost for barrier maintenance. The proposed barrier modeling approach is also with the potential to be implemented for quantitative and semi-quantitative risk assessment of various accident scenarios in terms of safety and security due to its flexibility and scalability and further facilitates barrier management.

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.

Acknowledgements

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

References

Abdo, H., Kaouk, M., Flaus, J.M., Masse, F., 2018. A safety/security risk analysis approach of Industrial Control Systems: a cyber bowtie–combining new version of attack tree with bowtie analysis. Comput. Secur. 72, 175–195.

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.

Argenti, F., Landucci, G., Cozzani, V., Reniers, G., 2017. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Saf. Sci. 94, 181–196.

Basri, E.I., Razak, I.H.A., Ab-Samat, H., Kamaruddin, S., 2017. Preventive maintenance (PM) planning: a review. J. Qual. Maint. Eng. 23, 114–143.

Bellamy, L., Oh, J.I.H., Hale, A.R., Papazoglou, I.A., Ale, B.J.M., Morris, M., Aneziris, O., Post, J.G., Walker, H., Brouwer, W.G.J. & Muyselaar, A.J. , 1999. I-RISK development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks. Final Project Report ENVA-CT96–0243.

Bernsmed, K., Frøystad, C., Meland, P.H., Nesheim, D.A., Rødseth, Ø.J., 2017. Visualizing cyber security risks with bow-tie diagrams. In: Proceedings of the International Workshop on Graphical Models for Security. Springer, Cham, pp. 38–56 (August).

Bucelli, M., Paltrinieri, M.N., Landucci, G., & Cozzani, V. , 2017. Safety barrier management and risk assessment: integration for safer operations in the Oil&Gas industry. In Proceedings of the Hazards 27, Symposium Series No 162, IChemE.

Caputo, A.C., Pelagagge, P.M., Palumbo, M., 2011. Economic optimization of industrial safety measures using genetic algorithms. J. Loss Prev. Process Ind. 24 (5), 541–551.

CCPS/EI, 2018. Bow Ties in Risk Management, Center for Chemical Process Safety and Energy Institute (UK). Wiley - AIChE, New York.

Çetinkaya, E.K. , 2001. Reliability Analysis of SCADA Systems Used in the Offshore Oil and Gas Industry.

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., 2019. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach. Reliab. Eng. Syst. Saf. 191, 106470.
Chen, C., Reniers, G., Khakzad, N., 2021a. A dynamic multi-agent approach for modeling the evolution of multi-hazard accident scenarios in chemical plants. Reliab. Eng. Syst. Saf. 207, 107349.
Chen, C., Reniers, G., Khakzad, N., Yang, M., 2021b. Operational safety economics: foundations, current approaches and paths for future research. Saf. Sci. 141, 105326.
De Dianous, V., Fievez, C., 2006. ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. J. Hazard. Mater. 130 (*3*), 220–233.
Debray, B., Piatyszek, E., Cauffet, F., Londiche, H. , 2004. Appendix 7: frequencies and probabilities data for the fault tree. ARAMIS project D1C.
de Ruijter, A., Guldenmund, F., 2016. The bowtie method: a review. Saf. Sci. 88, 211–218.
Dimaio, F., Scapinello, O., Zio, E., Ciarapica, C., Cincotta, S., Crivellari, A., Larosa, L., 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.
Eisinger, S., Rakowsky, U.K., 2001. Modeling of uncertainties in reliability centered maintenance—a probabilistic approach. Reliab. Eng. Syst. Saf. 71 (*2*), 159–164.
Fiorentini, L., Marmo, L., 2018. Sound barriers management in process safety: bow-tie approach according to the first official AIChE-CCPS Guidelines. Chem. Eng. Trans. 67, 253–258.
Freeman, R.A., 1990. CCPS guidelines for chemical process quantitative risk analysis. Plant/Oper. Prog. 9 (*4*), 231–235.
Goldberg, D.E., 1989. Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley, USA.
Gravestock, N. , 2008. Effectiveness of Fire Safety Systems for Use in Quantitative Risk Assessments, New Zealand Fire Service Commission, Wellington, NZ.
Guzman, N.H.C., Kozine, I., Lundteigen, M.A., 2021. An integrated safety and security analysis for cyber-physical harm scenarios. Saf. Sci. 144, 105458.
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., Håbrekke, S., Lundteigen, M.A. , 2010. Reliability Prediction Method for Safety Instrumented Systems–PDS Example collection, 2010 ed., SINTEF Report A, 17956, 42–50.
Hauge, S., Onshus, T. , 2010. Reliability Data for Safety Instrumented Systems PDS Data Handbook, 2010 ed., SINTEF Report A, 13502.
Hosseinnia Davatgar, B., Paltrinieri, N., Bubbico, R., 2021. Safety barrier management: risk-based approach for the oil and gas sector. J. Mar. Sci. Eng. 9 (*7*), 722.
Iaiani, M., Tugnoli, A., Cozzani, V., 2022. Identification of reference scenarios for security attacks to the process industry. Process Saf. Environ. Prot. 161, 334–356.
IEC, 2016. Functional Safety – Safety Instrumented Systems for the Process Industry Sector, Gen`eve, Switzerland (IEC).
Ji, Z., Yang, S.H., Cao, Y., Wang, Y., Zhou, C., Yue, L., Zhang, Y., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf. Environ. Prot. 148, 1279–1291.
Johansen, I.L., Rausand, M., 2015. Barrier management in the offshore oil and gas industry. J. Loss Prev. Process Ind. 34, 49–55.
Jovanovic, A., 2003. Risk-based inspection and maintenance in power and process plants in Europe. Nucl. Eng. Des. 226 (*2*), 165–182.
Khakzad, N., Khan, F., Amyotte, P., 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Saf. Environ. Prot. 91 (*1–2*), 46–53.
Kirwan, B., 2017. A Guide to Practical Human Reliability Assessment. CRC Press.
Landucci, G., Argenti, F., Cozzani, V., Reniers, G., 2017. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Saf. Environ. Prot. 110, 102–114.
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.
Lees, F.P. , 1980. Loss Prevention in the Process Industries, Butterworth Hienemann Ltd, Oxford, ISBN 0-7506-1529-X, 625.
Lewis, S., 2005. An overview of leading software tools for QRA. Am. Soc. Saf. Eng. East 18–22.
Mathworks-Genetic algorithm. (n.d.). Retrieved September 28, 2022. ⟨https://nl.mathworks.com/help/gads/genetic-algorithm.html⟩.
OREDA, 2002. Offshore Reliability Data Handbook. DNV, Trondheim, Norway.
Ottermo, M., Hauge, S., Håbrekke, S., 2021. Reliability Data for Safety Equipment: PDS Data Handbook. SINTEF Technology and Society, Trondheim.
Ouache, R., Kabir, M.N., Adham, A.A., 2015. A reliability model for safety instrumented system. Saf. Sci. 80, 264–273.
Paltrinieri, N., Tugnoli, A., Buston, J., Wardman, M., Cozzani, V., 2013. Dynamic procedure for atypical scenarios identification (DyPASI): a new systematic HAZID tool. J. Loss Prev. Process Ind. 26 (*4*), 683–695.
Papazoglou, I.A., Bellamy, L.J., Hale, A.R., Aneziris, O.N., Ale, B.J.M., Post, J.G., Oh, J.I. H., 2003. I-Risk: development of an integrated technical and management risk methodology for chemical installations. J. Loss Prev. Process Ind. 16 (*6*), 575–591.
Pishro-Nik, H. , 2016. Introduction to Probability, Statistics, and Random Processes.
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.
Redutskiy, Y., 2017. Optimization of safety instrumented system design and maintenance frequency for oil and gas industry processes. Manag. Prod. Eng. Rev. 8, 46–59.
Reniers, G.L., Van Erp, H.N., 2016. Operational Safety Economics: a Practical Approach Focused on the Chemical and Process Industries. John Wiley & Sons.
Schmitz, P., Swuste, P., Reniers, G., van Nunen, K., 2020. Mechanical integrity of process installations: barrier alarm management based on bowties. Process Saf. Environ. Prot. 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.
Selvik, J.T., Aven, T., 2011. A framework for reliability and risk centered maintenance. Reliab. Eng. Syst. Saf. 96 (*2*), 324–331.
Song, G., Khan, F., Yang, M., 2019a. Integrated risk management of hazardous processing facilities. Process Saf. Prog. 38 (*1*), 42–51.
Song, G., Khan, F., Yang, M., 2019b. Probabilistic assessment of integrated safety and security related abnormal events: a case of chemical plants. Saf. Sci. 113, 115–125.
Tan, Z., Li, J., Wu, Z., Zheng, J., He, W., 2011. An evaluation of maintenance strategy using risk based inspection. Saf. Sci. 49 (*6*), 852–860.
Taylor, J.R. (2010). The QRAQ Project Volume 4: Frequency of Releases and Accidents. ⟨https://www.academia.edu/35376294/The_QRAQ_Project_Volume_4_Frequency_of_Releases_and_Accidents⟩. (Accessed May 2022).
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.
Wang, Y., Cai, B., Zhang, Y., Liu, J., Khan, J.A., Liu, Y., Liu, Y., 2022. Condition-based maintenance method for multicomponent system considering maintenance delay based on remaining useful life prediction: subsea tree system as a case. Ocean Eng. 266, 112616.
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.
Xie, C., Huang, L., Wang, R., Deng, J., Shu, Y., Jiang, D., 2022. Research on quantitative risk assessment of fuel leak of LNG-fuelled ship during lock transition process. Reliab. Eng. Syst. Saf., 108368
Yang, S.H., Cao, Y., Wang, Y., Zhou, C., Yue, L., Zhang, Y., 2021. Harmonizing safety and security risk analysis and prevention in cyber-physical systems. Process Saf. Environ. Prot. 148, 1279–1291.
Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Del Prete, E., 2022. Integrated management of safety and security in Seveso sites-sociotechnical perspectives. Saf. Sci. 151, 105741.
Yuan, S., Cai, J., Reniers, G., Yang, M., Chen, C., Wu, J.. 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., Reniers, G., Yang, M., 2022b. The necessity of integrating safety and security barriers in the chemical process industries and its potential framework. Chem. Eng. Trans. 91, 13–18.
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.
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. Prot. 134, 149–160.
Zhen, X., Han, Y., Huang, Y., 2021. Optimization of preventive maintenance intervals integrating risk and cost for safety critical barriers on offshore petroleum installations. Process Saf. Environ. Prot. 152, 230–239.