TU Delft

Delft University of Technology

Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants

Yuan, Shuaiqi; Yang, Ming; Reniers, Genserik

DOI
10.1016/j.compind.2023.104056

Publication date
2023

Document Version
Final published version

Published in
Computers in Industry

Citation (APA)
Yuan, S., Yang, M., & Reniers, G. (2023). Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants. *Computers in Industry*, *155*, Article 104056. https://doi.org/10.1016/j.compind.2023.104056

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.

This work is downloaded from Delft University of Technology.
For technical reasons the number of authors shown on this cover page is limited to a maximum of 10.

Computers in Industry 155 (2024) 104056

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.sciencedirect.com/journal/computers-in-industry

Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants

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

[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, K`ULeuven, 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 and security risks
Cyber-to-physical attacks
Probabilistic risk assessment
Cyber-physical systems
Bow-tie diagram
Bayesian network

ABSTRACT

Aligned with the development needs of Industry 4.0, industrial cyber-physical systems (ICPSs) are widely applied to chemical facilities to facilitate so-called intelligent production processes. Meanwhile, emerging cyber-to-physical (C2P) risks are introduced due to the vulnerability of ICPSs to cyberattacks. An integrated safety and security risk assessment of chemical facilities equipped with industrial cyber-physical systems becomes challenging, particularly in performing a probabilistic/quantitative risk assessment. Targeting this gap, this study develops a systematic approach to construct accident scenarios concerning both safety hazards and security threats and performs a probabilistic risk assessment of chemical facilities considering the interdependency between safety-associated events and security-associated events. In the proposed approach, bow-tie technique is used to perform a safety risk analysis, and meanwhile, the possible dangerous scenarios caused by physical attacks and C2P attacks are also identified and integrated into the bow-tie diagram. Particularly, attack impact modeling of C2P attacks helps to identify dangerous attack modes, and a time-to-compromise (TTC) based method is used to quantify the vulnerability of ICPSs to C2P attacks. Then, a Bayesian network (BN) model is developed to perform an integrated safety and security risk analysis. An illustrative case study is used in this study to give guidance on performing integrated safety and security risk assessment of ICPSs and validate the feasibility of the proposed approach.

1. Introduction

With the advent of the digital age and Industry 4.0, new threats and risks have emerged in the chemical process industries. For instance, integrating digital technologies into traditional process operations increases the systems' complexity and introduces new security vulnerabilities in many cases (Kriaa et al., 2015). One of the major concerns is the implementation of industrial cyber-physical systems (ICPSs) that may induce damage to the physical world due to their vulnerabilities subject to cyberattacks (Ji et al., 2021). Previous studies show that a cyberattack on an ICPS may adversely impact physical components and further cause damage to humans, assets, and the environment (Kriaa et al., 2015; Huang et al., 2018). The corresponding risks are known as cyber-to-physical (C2P) risks (Yampolskiy et al., 2013). As a result, chemical facilities are exposed to multi-dimensional risks associated with major accident scenarios (fires, explosions, toxic leakage, etc.). Major accident associated risks can be categorized as follows:

- i) Safety risks affiliated with safety hazards/causes, including accidental technical component failures, human errors, external interventions, etc.
- ii) Physical security risks affiliated with intentional attacks/malicious acts aiming to exploit the vulnerability of physical elements (usually not including information systems).
- iii) Cyber-to-physical (C2P) risks affiliated with intentional attacks/malicious acts aiming to impact physical elements by exploiting the vulnerability of cyber elements (usually through attacks on information systems).

* 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.compind.2023.104056
Received 1 July 2023; Received in revised form 16 October 2023; Accepted 19 November 2023
Available online 30 November 2023
0166-3615/© 2023 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

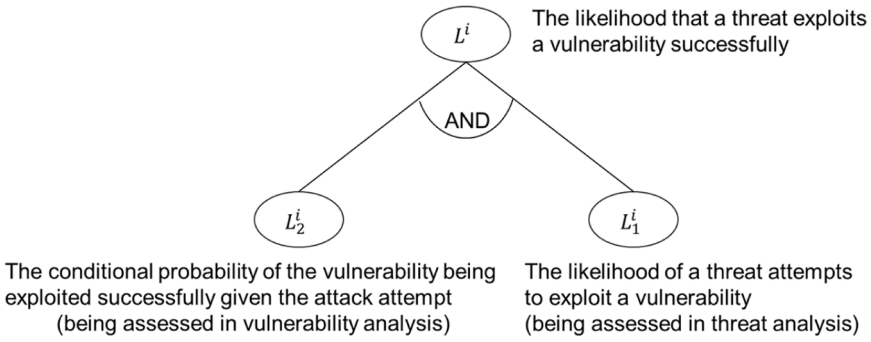


Fig. 1. Probabilistic calculation based on an attack tree analysis.

Those risks inevitably interact because security-related events may influence safety-related events and vice versa. For example, intentional attacks on safety barriers may increase safety risks due to the loss of protection function (of the safety barriers). Also, specific safety barriers may be regarded as mitigative barriers to security threats, which can mitigate consequences caused by intentional attacks (Yuan et al., 2022).

Previous studies show systemic risks are poorly understood in practice because security risk analyses and safety risk analyses are often undertaken independently in Seveso sites (Ylönen et al., 2022). Several attempts at integrating safety and physical security risk assessment in chemical plants were made by researchers. For instance, Casciano et al. (2019) developed an algorithm for ranking chemical industrial clusters with respect to safety and security risks. Chen et al. (2019) proposed a dynamic graph approach to integrate safety and security resources to reduce the risk of man-made domino effects. Moreno et al. (2022) assessed escalating scenarios in process plants considering the combined contribution of safety and security barriers. Yuan et al. (2023b) proposed an approach for determining optimal maintenance intervals for safety barriers considering both accidental and intentional adverse scenarios. However, those studies haven't addressed the integrated safety and security risk assessment of ICPSs in chemical plants.

Regarding the safety and security of ICPSs, bow-tie diagrams are considered capable of visualizing accident scenarios in terms of safety, physical security, and cybersecurity (Abdo et al., 2018; Ji et al., 2021). Abdo et al. (2018) combined bow-tie diagrams and attack trees to demonstrate adverse scenarios of industrial control systems (ICSs) considering safety hazards and security threats. Guzman et al. (2020) suggested using a multi-layered representation for safety and security analysis of CPSs considering information flows and energy flows. Additionally, as an extension of the system theoretic process analysis (STPA) approach, STPA-SafeSec was developed and implemented for safety and security analysis of cyber-physical systems (Friedberg et al., 2017). Alanen et al. (2022) proposed an ontology-based approach for cybersecurity risk analysis of ICSs. Huang et al. (2018) combined Bayesian network (BN) and stochastic hybrid system (SHS) to quantify the physical impact of cyberattacks on ICPSs.

However, to the best of the authors' knowledge, the research on quantitative risk assessment of chemical facilities considering the interdependency between safety risks, physical security risks, and C2P risks is still lacking. Because both safety hazards and security threats could lead to major accident consequences, the consideration of only safety hazards or security threats could lead to a risk underestimation. Meanwhile, separate assessments of safety-associated scenarios and security-associated scenarios cannot reveal the real risks due to the ignorance of the interdependency between safety and security. Targeting this gap, this study provides a systematic approach for risk assessment of ICPSs in chemical plants considering the interdependency and interactions between safety-hazard-induced adverse events and security-threat-induced adverse events. The remainder of this paper is organized as follows. Firstly, the research scope of interest is well identified and the safety and security risk calculations are presented in Section 2. Then, the proposed approach is illustrated in Section 3 while an illustrative case study is used to theoretically validate the feasibility of the proposed approach in Section 4. Discussions and conclusions are presented in Section 5 and Section 6, respectively.

2. Theoretical background

Typically, studies associated with unintentional or random losses (due to hazards) are considered to belong to the safety domain. In contrast, studies related to intentional losses and with deliberate nature (deliberate misuse of hazards) belong to the security domain (Landucci et al., 2020). The integration of safety and security was highly stressed to promote the third safety revolution (represented by the acronym CHESS) in the chemical process industries by Reniers and Khakzad (2017), in which security is suggested to be treated in an integrated way with safety by company safety management. With cyber-physical (C2P) attacks getting more and more attention, the investigation of the physical damages induced by cyberattacks becomes important (Flaus, 2019). Aligned with the promotion of safety and security integration, all kinds of causes (safety hazards, physical attacks/acts, and cyber-physical attacks) leading to major accident scenarios (fires, explosions, toxic leakage, etc.) should be covered in the risk assessment to generate more physically dangerous scenarios and to serve more thorough risk analysis.

In the safety science domain, risk is widely presented as a function of the likelihood of an unwanted scenario i (presented by L^i) and its expected consequence severity, S^i, as follows (Freeman, 1990; Meyer and Reniers, 2022):

$$R^i_{safety} = L^i \times S^i \tag{1}$$

Regarding security risks, the API standard 780 (API, 2013) defined security risk as a function of the consequences (C^i) of a successful attack scenario i and the likelihood (L^i) of the happening of this successful attack scenario. The likelihood is further defined as a function of the attractiveness (A^i) to the adversary of the asset, the degree of threat (T^i) posed by the adversary, and the degree of vulnerability (V^i) of the asset. According to the IEC 62443–3–2 standard (IEC, 2020), which particularly serves the information security of ICSs, the cybersecurity risk is expressed as the likelihood (L^i) that a particular threat will exploit a particular vulnerability with a particular consequence (C^i). With the consideration of the above two definitions, security risks can be calculated as follows (Landucci et al., 2020):

$$R^i_{security} = L^i \times C^i = (A^i \times T^i) \times V^i \times C^i = L^i_1 \times L^i_2 \times C^i \tag{2}$$

where L^i_1 is the likelihood of an attempt to exploit a vulnerability. L^i_2 presents the conditional probability of the vulnerability being exploited successfully given the attack attempt. Usually, L^i_1 should be evaluated in the threat analysis. L^i_2 reflects the vulnerability of the targeted system posed to attacks, and it is usually addressed in the vulnerability

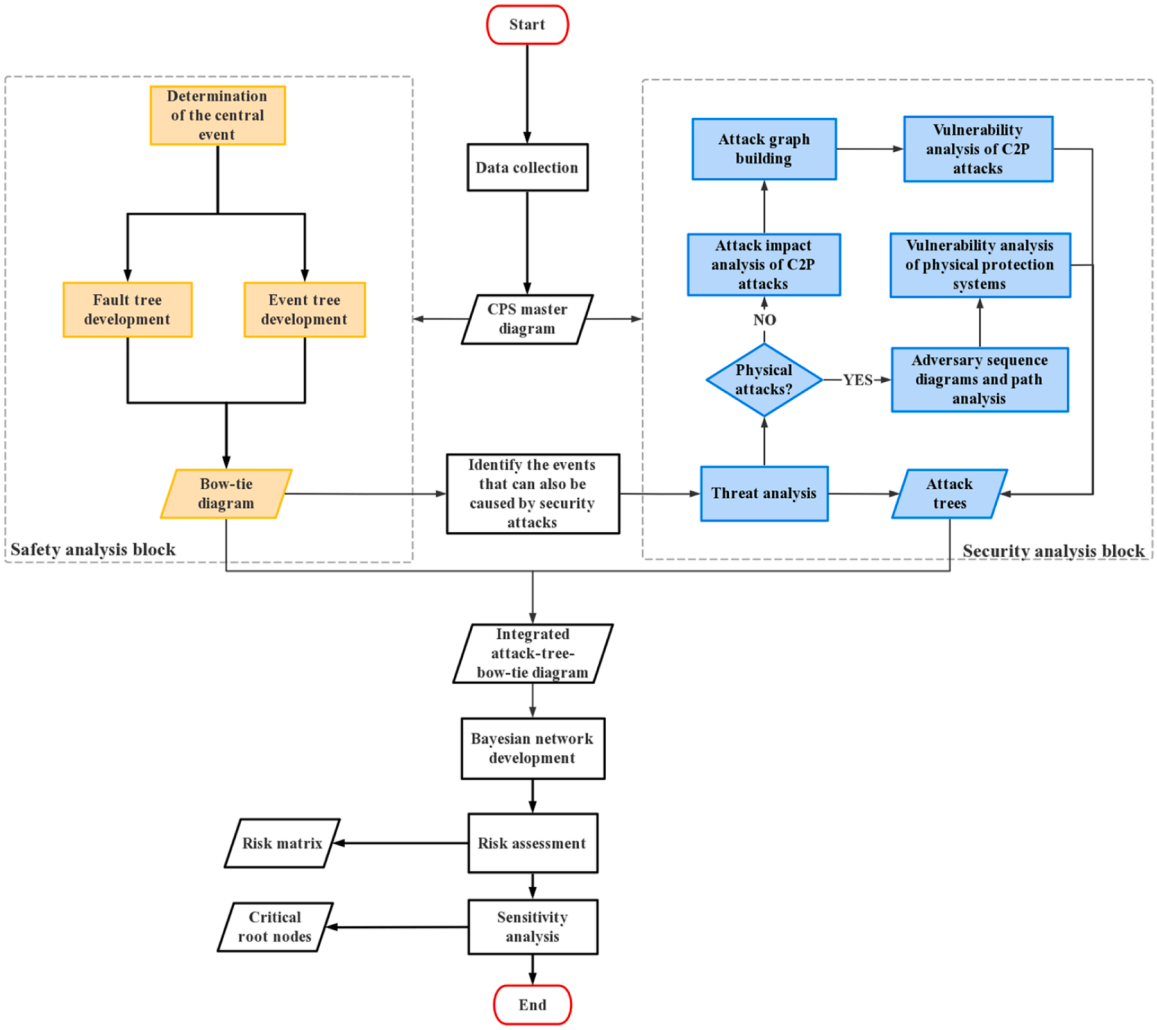


Fig. 2. Flowchart of the proposed methodology.

assessment. We demonstrate how to calculate security risks based on an attack tree analysis, as shown in Fig. 1.

3. Methodology

3.1. Overview of the proposed approach

The workflow of the proposed approach is organized in a systematic manner, as presented in Fig. 2. The proposed approach starts with system representation using a CPS master diagram, and then, safety analysis and security analysis are conducted to generate an integrated attack-tree-bow-tie diagram. Furthermore, a BN model is developed with the integration of safety-associated and security-related scenarios for risk assessment. The following subsections illustrate the details of each step of the proposed approach.

3.2. System representation and CPS master diagrams

The system complexities of ICPS bring enormous difficulties to safety analysis and security analysis. As a result, an appropriate representation of the ICPSs should serve as a basis for safety analysis, security analysis, and their corresponding scenario building. Guzman et al. (2020) suggested using a multi-layered representation of CPSs for an integrated safety and security analysis. A tool named CPS master diagram was proposed by the same study, in which the CPS is represented by three layers (physical layer, cyber-physical layer, and cyber layer) with the illustration of the information/data flow and energy flow between different components and between the CPS and external environments. An exemplary CPS master diagram is presented in Fig. 3.

3.3. Safety risk analysis based on bow-tie diagrams

As a graphical tool, bow tie diagrams are widely used for accident scenario identification and visualization due to their advantage of being straightforward to communicate to a wide range of audiences (CCPS/EI, 2018). The development of a bow-tie diagram usually begins with the determination of the central event. Then, a fault tree considering the possible causes of the central events should be constructed based on the energy flows and information flows presented in the CPS master diagram. Typically, the basic events in the fault tree include technical component failures, human errors, external interventions, etc. The occurrence probabilities of those events can be derived from reliability databases (OREDA, 2002; Hauge and Onshus, 2010), human reliability data (Kirwan, 2017), accident databases (Debray et al., 2004), or data available in the literature. Meanwhile, an event tree considering the possible consequences after the occurrence of the central event should be developed with the help of the available guidelines. For instance, the ARAMIS project (Andersen et al., 2004) provided methods for constructing event trees with respect to major accident hazards in chemical plants. Vílchez et al. (2011) provided a set of generic event trees considering the release of hazardous materials in chemical plants.

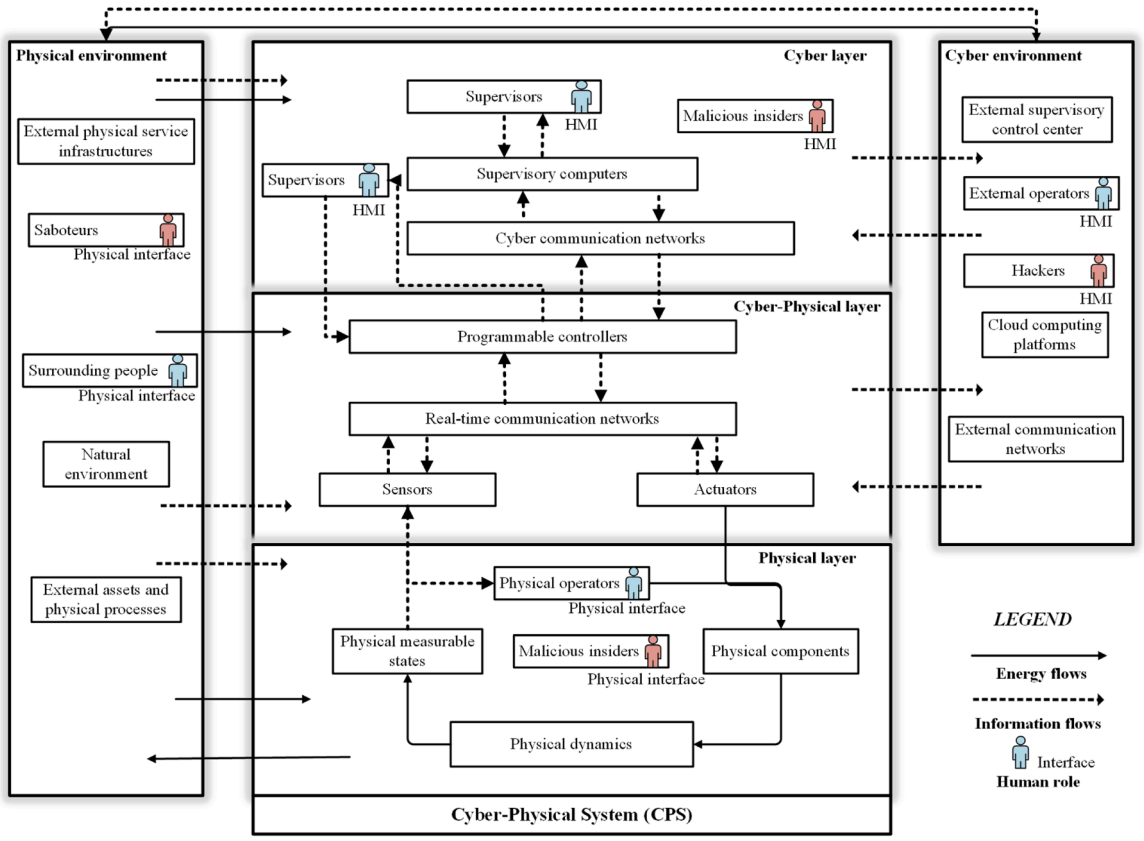


Fig. 3. An exemplary CPS master diagram, adapted from Guzman et al. (2020).

3.4. Security risk analysis

3.4.1. Threat analysis

Security risk analysis begins with a threat analysis aiming to identify threat agents who may execute physical attacks or C2P attacks. It is suggested to identify potential threat agents of the targeted chemical facilities by asking who can conduct attacks and why. The approach suggested by SFK (2002) is adopted to identify threat agents' categories (TAC), as shown in Table 1.

Threat analysis also addresses the estimation of attack likelihoods, which correspond to L_1 in Fig. 1. It is suggested to estimate attack likelihoods according to the actual annual frequency of attacks in the investigated chemical plants or refer to similar companies in the same/similar sector. However, not many companies revealed the security attack information due to confidential issues. Alternatively, a simplified frequency estimation of physical attacks can be implemented based on the API threat levels and facility expected life according to (API, 2013) and (Landucci et al., 2017), as presented in Table 2.

Regarding C2P attacks, attack likelihood may be estimated by analyzing the cyber incidents related to the investigated chemical facility or comparable industrial facilities. According to the statistical analysis of 60767 cyber security incidents that occurred in the US from November 2008 to January 2015 (Kuypers and Maillart, 2018), it was observed that the recurrence intervals of larger events remain overall stable. The recurrence intervals of cyber security incidents with different severities, which are measured in the form of efforts (man-hours) spent remediating the incidents, are given in Table 3 (Kuypers and Maillart, 2018). With reference to the results presented in Table 3, the recurrence interval of C2P attacks is estimated at approximately 150–465 days. In case no incident data is available, security experts may estimate the attack likelihood based on their own knowledge and experience. Because how to improve the expert judgment/elicitation on attack

Table 1
Definitions of threat agent categories (TAC) according to SFK (2002).

Features	TAC1: threat agent moved by contingent intent	TAC2: threat agent moved by direct intent	TAC3: terrorists and extremists
Agents	Individuals or small groups	Small network of activists, members of organized crime, individuals, radical political groups	Extremist and terrorist individuals and groups
Aim	Limited damage; possible unawareness of attack escalation into major accident	Major damage; escalation into a major accident may be a possible objective	Massive terrorist attack, armed action, causing the maximum possible damage, without regard to people's life (own or others)
Motivation	Revenge, frustration, prove existence of deficits, achieve social effects	Revenge, political radicalism, gaining financial/competitive advantages	Religion related motives, anarchy, "punishing companies"
Potentiality	Limited potentiality, dependent on the motive	Above average criminal energy, average communication capability, medium level of organizational support, poor financial backing	Extremely great criminal energy, highly developed communication capability, high level of organizational support, high financial backing
Tools and means	Simple or major tools, possibly simple incendiary devices	Simple and specialized tools, incendiary devices, home-made explosives	Simple and heavy tools, weapons, explosives, incendiary devices

Table 2
Attack annual probability estimation based on the API threat level and facility expected life (Λ, in year), adapted from API (2013) and Landucci et al. (2017).

API threat level	Description	Attack annual probability
1	Little or no credible evidence of capability or intent, and no history of actual or planned threats against the facility.	$10^{-1} \times 1/\Lambda$
2	Low threat against the facility, few known adversaries would pose a threat to the asset.	$1/\Lambda$
3	Medium threat level, possible threat's desire to compromise similar assets, but no specific threat exists for the facility under analysis.	1×10^{-1}
4	A credible threat exists against the facility based on the knowledge of the threat's capability and intent to attack similar assets and some indication exists of the threat specific to the company, facility or asset.	2×10^{-1}
5	Some credible threat exists against the facility and the threat demonstrates the capability and intent to launch an attack; similar assets are attacked on a frequently recurring base and the frequency of attack is very high.	6×10^{-1}

Table 3
Recurrence intervals of cyber security incidents with different severities, adapted from Kuypers and Maillart (2018).

Effort spent to remediate incident (man-hours)	Recurrence intervals (days)	Effort spent to remediate incident (man-hours)	Recurrence intervals (days)
>6	2.99	>48	41.87
>12	8.02	>168	153.91
>24	24.17	>720	465.97

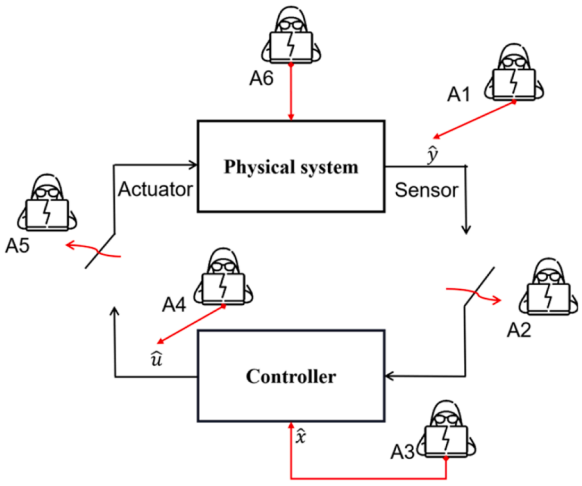


Fig. 4. Typical attacks against industrial PLCs, adapted from Huang et al. (2009), Wen et al. (2023).

likelihood estimation is without the scope of this study, the appropriate handling of subjectivity in the attack likelihood estimation is not addressed in this study. Future studies may focus on the improvement of attack likelihood estimation considering the treatment of subjectivity.

3.4.2. Vulnerability analysis with respect to physical attacks

Vulnerability assessment aims to identify credible attack paths and estimate the conditional probability of successful attacks given the attack attempts (corresponding to L_2 in Fig. 1). For physical attacks, the attacks are usually subject to PPSs (physical protection systems). A systematic approach should be implemented to identify credible attack paths with the consideration of the physical protection systems, for instance, fences, entry control, closed circuit television (CCTV), emergency team, and so on (Reniers et al., 2017). An Adversary Sequence Diagram (ASD) is a graphical representation of physical protection system elements along attack paths that adversaries may follow to accomplish their objectives. This paper adapts Adversary Sequence Diagrams and Path Analysis to identify the credible attack paths of physical attackers. Details of Adversary Sequence Diagrams and Path Analysis can be found in Norman (2010). After the credible attack paths are identified, the methodology and benchmark data presented by Moreno et al. (2022) are adapted for vulnerability assessment of PPSs using an event tree analysis. An example of the vulnerability assessment of PPSs can be found in Appendix I.

3.4.3. Identification of dangerous C2P attack modes

Regarding C2P attacks, the ultimate attack targets of attackers are usually physical components of the CPS. Because industrial PLCs (programmable logic controllers) are usually used to control the physical dynamics of chemical facilities, industrial PLCs become the main targets for attackers aiming to execute C2P attacks. Fig. 4 demonstrates six types of typical attacks against industrial PLCs. The explanation of those attack types is given in Table 4.

The successful implementation of C2P attacks is not always capable of inducing dangerous scenarios, instead, some of those attacks only cause some deviations that the control system can suppress (Huang et al., 2009; Cárdenas et al., 2011). Therefore, it is necessary to perform an attack impact analysis of all possible C2P attack modes and to identify dangerous attack modes. For C2P attacks against sensors, let $y_i(k)$ denotes the measurement by sensor i at time k, and the sensor measurement is always within its predefined range, $y_i(k) \in Q = [y_i^{\min}, y_i^{\max}]$. Let $\widetilde{y}_i(k)$ denotes the received measurement by the controller at time k. If this sensor is under attack, $\widetilde{y}_i(k)$ may be different from the real measurement $y_i(k)$, as follows (Cárdenas et al., 2011):

Table 4
Explanation of typical C2P attacks against industrial cyber-physical systems, adapted from Huang et al. (2009),Orojloo et al. (2017), Wen et al. (2023).

Marks	Attack types	Descriptions
A1	FDI (false data injection) attack against sensors	Maliciously manipulate the measurement data from sensors to the controller. Let $\hat{y} \neq y$, $\hat{y}$ is the manipulated data, and y is the true measurement.
A2	DoS (denial-of-service) attack against sensors	Maliciously prevent the controller from receiving sensor measurement data.
A3	Setpoint manipulation	Maliciously manipulate the setpoints configured in the controller. Let $\hat{x} \neq x$, $\hat{x}$ is the manipulated setpoint, and x is the predefined setpoint.
A4	FDI attack against actuators	Maliciously manipulate the control data from the controller to actuators. Let $\hat{u} \neq u$, $\hat{u}$ is the manipulated data, and u is the true control data.
A5	DoS attack against actuators	Maliciously prevent actuators from receiving control commands/data.
A6	Physical attack	Physical attacks against actuators or direct physical attacks on the vessels.

$$\widetilde{y}_i(k) = \begin{cases} y_i(k) & for \quad k \notin K \\ a_i(k) & for \quad k \in K \end{cases} \tag{3}$$

where $K = \{k_s, \ldots, k_e\}$ represents the attack duration between the attack start time k_s and the attack stop time k_e. $a_i(k)$ is the manipulated data by the attack. Because the manipulated measurement outside Q can be easily detected as a fault by the fault-tolerant algorithms, it is assumed that $a_i(k)$ also lies within Q (presented by $a_i(k) \in Q$). In the case of a DoS attack, a lack of measurement occurs during the attack. Consequently, the last received measurement will be used by the controller until new measurements are received after the DoS attack, as follows (Cárdenas et al., 2011):

$$a_i(k) = y_i(k_s), for \quad k \in K \tag{4}$$

where $y_i(k_s)$ is the last received measurement before the DoS attack starts. In terms of FDI attacks, attackers can inject any arbitrary value to manipulate the measurement data received by the controller. Thus, $a_i(k)$ can be any arbitrary value within the measurement range of the sensor. For instance, Min and Max Attacks, Scaling Attacks, and Additive Attacks are the possible methods implemented by attackers for FDI attacks, illustrated as follows (Huang et al., 2009):

i) Min and Max Attacks

$$a_i(k) = y_i^{\min}, for \quad k \in K; Min \quad attacks \tag{5}$$

and

$$a_i(k) = y_i^{\max}, for \quad k \in K; Max \quad attacks \tag{6}$$

ii) Scaling Attacks

$$a_i(k) = \begin{cases} \beta(t) y_i(k), for \quad k \in K \quad and \quad \beta(t) y_i(k) \in Y_i \\ y_i^{\min}, for \quad k \in K \quad and \quad \beta(t) y_i(k) \le y_i^{\min} \\ y_i^{\max}, for \quad k \in K \quad and \quad \beta(t) y_i(k) \ge y_i^{\max} \end{cases} \tag{7}$$

where $\beta(t)$ is the scale factor, which is a function of time t.

iii) Additive Attacks

$$a_i(k) = \begin{cases} y_i(k) + \gamma(t), for \quad k \in K \quad and \quad y_i(k) + \gamma(t) \in Y_i \\ y_i^{\min}, for \quad k \in K \quad and \quad y_i(k) + \gamma(t) \le y_i^{\min} \\ y_i^{\max}, for \quad k \in K \quad and \quad y_i(k) + \gamma(t) \ge y_i^{\max} \end{cases} \tag{8}$$

where $\gamma(t)$ is the scale factor, which is a function of time t. Similarly, the approach for modeling C2P attacks against sensors can also be adapted for C2P attacks against actuators, as follows (Huang et al., 2009):

$$\widetilde{u}_i(k) = \begin{cases} u_i(k) & for \quad k \notin K \\ a_i(k) & for \quad k \in K \end{cases} \tag{9}$$

where $u_i(k)$ is the correct control data from the controller to actuator i at time k. $\widetilde{u}_i(k)$ is the control data received by the actuator at time k. When the actuator is under C2P attacks ($k \in K$), the manipulated signal ($a_i(k)$) will be used by the actuator instead of the correct control data $u_i(k)$. $a_i(k)$ in Eq. (9) can also be calculated following the same methods presented by Eq. (4) to Eq (8) with the replacement of sensor measurement y to control data u. A detailed illustration of the approach for impact analysis of FDI attacks and DoS attacks can be found in (Huang et al., 2009).

For setpoint manipulations, the setpoint used by the controller may be modified by attackers as any arbitrary value ($a_i(k)$), as follows (Wen et al., 2023):

$$\widetilde{s}_i(k) = \begin{cases} s_i & for \quad k \notin K \\ a_i(k) & for \quad k \in K \end{cases} \tag{10}$$

where s_i is the predefined setpoint value. $\widetilde{s}_i(k)$ is the setpoint value used by the controller at time k. By integrating the above attack modeling into a system control model, the system state vector with n variables ($X = \{x_1, \ldots, x_n\}$) under the influence of C2P attacks can be evaluated, as demonstrated below.

$$\begin{cases} X(k+1) = f(X(k), \widetilde{U}(k), w) \\ Y(k) = g(X(k), v) \\ U(k) = h(\widetilde{S}(k), \widetilde{Y}(k)) \end{cases} \tag{11}$$

where $X(k+1)$ is the system state vector at time $k+1$, which depends on $X(k)$, the control actions of l actuators, $\widetilde{U}(k)=\{\widetilde{u}_1(k), \ldots, \widetilde{u}_l(k)\}$, and the process noise (w). $Y = \{y_1, \ldots, y_m\}$ is the observation vector composed of the observation data of m variables. $Y(k)$ depends on the system state vector, $X(k)$, and the observation noise (v). $U(k) = \{u_1(k), \ldots, u_l(k)\}$ is the control data for actuators, which depends on the j setpoint values, $\widetilde{S}(k) = \{\widetilde{s}_1(k), \ldots, \widetilde{s}_j(k)\}$, and the observed data from sensors ($\widetilde{Y}(k)=\{\widetilde{y}_1(k), \ldots, \widetilde{y}_m(k)\}$). $\widetilde{Y}(k)$, $\widetilde{U}(k)$, and $\widetilde{S}(k)$ are modeled using Eq. (3) to Eq (10) according to the specific attack modes and are used to estimate the system state vector. If we define a safety range for each system state variable, $R = \begin{bmatrix} x_1^{\min}, & x_1^{\max} \\ \ldots & \\ x_n^{\min}, & x_n^{\max} \end{bmatrix}$, a dangerous system state is induced by a C2P attack when $X(k) \notin R$ and $k \in K$. Therefore, the attack modeling helps to decide if a dangerous phenomenon can be induced by certain C2P attack modes based on the estimation of the system state vector. We demonstrate the application of the attack impact modeling in Section 4.2.2. Additionally, we introduce a coefficient, β, to depict the likelihood of a physically dangerous scenario that may be induced by a specific attack mode, as follows.

$$\beta = \Pr\{X(k) \notin R\}, k \in K \tag{12}$$

where $\Pr\{X(k) \notin R\}$ is the probability of $X(k) \notin R$ regarding a specific attack mode. $X(k)$ is estimated by using Eq. (11). $X(k)$ depends on $\widetilde{U}(k)$, $\widetilde{S}(k)$, $\widetilde{Y}(k)$, w and v, and attack modes impact the configuration of $\widetilde{U}(k)$, $\widetilde{S}(k)$ and $\widetilde{Y}(k)$. As a result, attack modes, process noise, and observation noise may impact the value of β. The determination of β for a specific attack mode should be conducted based on the attack modeling of this attack mode and also with the consideration of the impact of process noise and observation noise. We demonstrate an example of the determination of β for several attack modes in Section 4.2.2.

3.4.4. Vulnerability analysis with respect to C2P attacks

Regarding the identified dangerous attack modes (as illustrated in Section 3.4.3), the CPS master diagram and attack/compromise graph are combined to identify and visualize the possible attack paths. This process starts with the identification of the possible PoAs (points of access), which are usually the interfaces between the attackers and the cyber-physical system presented in the CPS master diagrams. Then, each attack step executed by the attackers starting from the PoAs to achieve their final attack target (which is usually the compromise of physical components) may be analyzed based on the information flows and control flows demonstrated in the CPS master diagram. Additionally, ICS vulnerability databases, for instance, an ICS-specific vulnerability dataset (Thomas and Chothia, 2020), may be used to identify the known vulnerabilities that may be exploited by attackers at each attack step. Finally, the implementation of an attack/compromise graph helps to visualize the attack paths for each attack mode considering the attack steps and vulnerabilities along the attack paths (Semertzis et al., 2022). An example of the attack path analysis can be found in Section 4.2.3.

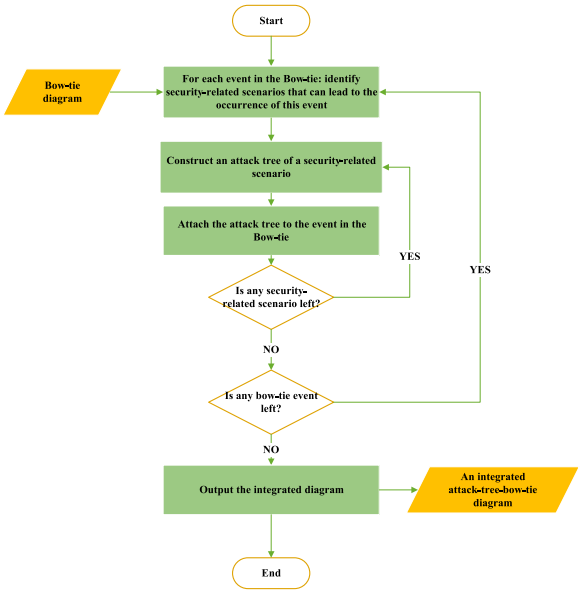


Fig. 5. Flowchart of integrating attack trees into the bow-tie diagram, adapted from Abdo et al. (2018).

Time-to-compromise (TTC) was defined as the time needed for an attacker to gain some levels of privilege on a system component by McQueen et al. (2006). In the same study, a TTC estimation approach was developed based on the Common Vulnerabilities and Exposures (CVEs) database (NVD, N.d.). Then, the TTC approach has been extended and applied to quantitative risk/reliability assessment of process control networks (Henry and Haimes, 2009) and power systems (Zhang et al., 2015; Semertzis et al., 2022). More recently, an updated/augmented TTC approach was developed particularly for ICSs (Ling and Ekstedt, 2022, 2023) based on an ICS-specific vulnerability dataset (Thomas and Chothia, 2020). This study adapts the approach developed by Ling and Ekstedt (2022) to estimate the TTC of each attack step considering attackers' skill levels, the number of known vulnerabilities in the attack step, and the exploitabilities of the known vulnerabilities. An illustration of the TTC estimation approach can be found in Appendix II. More details can be found in the original study (Ling and Ekstedt, 2022).

After the estimation of the TTC of each attack step, the global TTC of an attack path can be calculated by summing the TTC of each attack step along the attack path. For the target that can be accessed through multiple attack paths, the attack path with the shortest global TTC is used from a conservative point of view.

$$TTC_G(i) = \sum_{j=1}^{n} TTC_j \tag{13}$$

$$L^i = \frac{MTTD_i}{TTC_G(i) + MTTD_i} \times \beta_i \tag{14}$$

$$MTTD_i = \frac{\sum_{k=1}^{N} TTD_k}{N} \tag{15}$$

where $TTC_G(i)$ is the global TTC of an attack path *i*. TTC_j is the local TTC of attack step *j*. *n* is the number of attack steps along this attack path. The conditional probability of a C2P attack inducing physically dangerous scenarios successfully, L^i, can be estimated based on the global TTC ($TTC_G(i)$) and the mean-time-to-detect ($MTTD_i$) regarding this attack scenario, as shown in Eq. (14) (Semertzis et al., 2022). Mean-time-to-detect (MTTD) measures the average time it takes for the security operations center (SOC) to detect a security incident, which is one of the key metrics used to measure SOC performance (Mughal, 2022). The MTTD regarding a specific intrusion type is the sum of all incident detection times of this intrusion type ($\sum_{k=1}^{N} TTD_k$) divided by the total incident number of this intrusion type (*N*), as shown in Eq. (15). The MTTD values can be estimated based on the analysis of security incident data in practice. β_i is a coefficient depicting the likelihood of a physically dangerous scenario that may be induced by a successful intrusion of attack path *i*. β_i depends on the vulnerability of the OT (operational technology) system regarding specific C2P attack modes, and it is determined according to Section 3.4.3. Regarding the attacks that are not subject to intrusion detection systems (IDS), for instance, stealthy attacks (Hu et al., 2019), $L^i \approx \beta_i$ ($MTTD \approx +\infty$ in case of stealthy attacks) may be used instead of Eq. (14) because stealthy attacks are able to evade the detection of IDS and inject manipulated data into the control system.

3.5. Integrated safety and security risk analysis

3.5.1. Integrating attack trees into the bow-tie diagram

After threat analysis and vulnerability analysis, a simplified attack tree (like the attack tree in Fig. 1) for each attack mode should be developed, to incorporate the results from the threat analysis and vulnerability analysis. The simplified attack trees employ attack likelihoods (derived from threat analysis) and the conditional probabilities of successful attacks given attack attempts (derived from vulnerability analysis) to calculate the probability of successful execution of each attack mode without the demonstration of detailed attack paths and attack steps. Then, the developed attack trees are integrated with the bow-tie diagram for developing a BN model and for integrated safety and security risk assessment. This simplification of the attack trees helps to reduce the number of BN nodes effectively and meanwhile retain the necessary quantitative data for risk assessment. Particularly, regarding the assessment of large-scale facilities, complex attack paths may make the integrated safety and security risk analysis unachievable/unmanageable using BN models. The simplification of the attack tresses makes the BN model developing process easier and makes it possible to perform a risk assessment of large-scale facilities considering both safety-related and security-related scenarios.

Regarding the integration of safety-associated scenarios and security-related scenarios, a systemic workflow should be implemented to conduct scenario integration, as presented in Fig. 5. Basically, this can be done by checking if each event in the bow-tie diagram can also be induced by security attacks. If the answer is yes, the corresponding attack trees of the security attacks should be attached to the event.

3.5.2. Bayesian networks

Bayesian Networks (BNs) are widely-used to perform safety or security risk assessments (Tong et al., 2018; George and Renjith, 2021). Compared to conventional bow-ties and fault/attack trees, BN has the advantage of backward diagnostic analysis and handling dependent basic events and multiple occurrence events (Yuan et al., 2023a). Therefore, it is suggested to transform the obtained attack-tree-bow-tie diagram into a BN model for integrated safety and security risk analysis. A BN consists of a set of nodes, their correlations (represented by directed arcs), prior probabilities, and conditional probability tables (CPTs). A joint probability distribution $P(X)$ of variables $X = \{X_1, \ldots, X_n\}$ is presented in a BN as follows (Jensen and Nielsen, 2007):

$$P(X) = \prod_{i=1}^{n} P(X_i | Pa(X_i)) \tag{16}$$

where $Pa(X_i)$ is the parent node set of X_i. When evidence E becomes available, the posterior probabilities $P(X|E)$ can be calculated based on Bayes theorem as follows (Jensen and Nielsen, 2007):

$$P(X|E) = \frac{P(E|X) \bullet P(X)}{P(E)} = \frac{P(E,X)}{\sum_X P(E,X)} \tag{17}$$

Both the topology and CPTs of the BN model can be derived based on

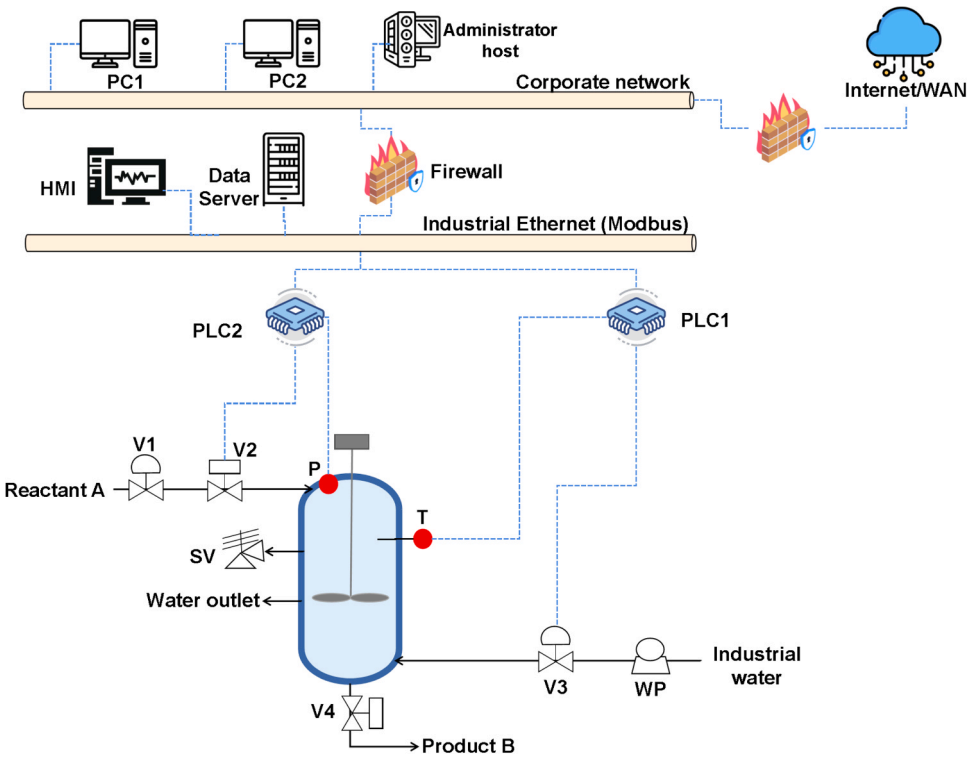


Fig. 6. The investigated chemical reactor with its SCADA system, adapted from Pilario and Cao (2018).

an integrated attack-tree-bow-tie diagram. Previous studies already illustrated the mapping process for transforming fault trees (Bobbio et al., 2001), attack trees (Gribaudo et al., 2015), and bow-tie diagrams (Khakzad et al., 2013) into BNs. Detailed procedures and guidelines can be found in related studies, this paper avoids repeating illustrations here.

3.5.3. Risk evaluation and sensitivity analysis

Risk evaluation should consider both the occurrence probabilities and severities of the undesired consequences. The BN model takes the responsibility to estimate the occurrence probabilities of the undesired consequences. Severities of the undesired consequences are determined based on qualitative severity classifications, for instance, the severity classes of typical dangerous phenomena defined in the ARAMIS project

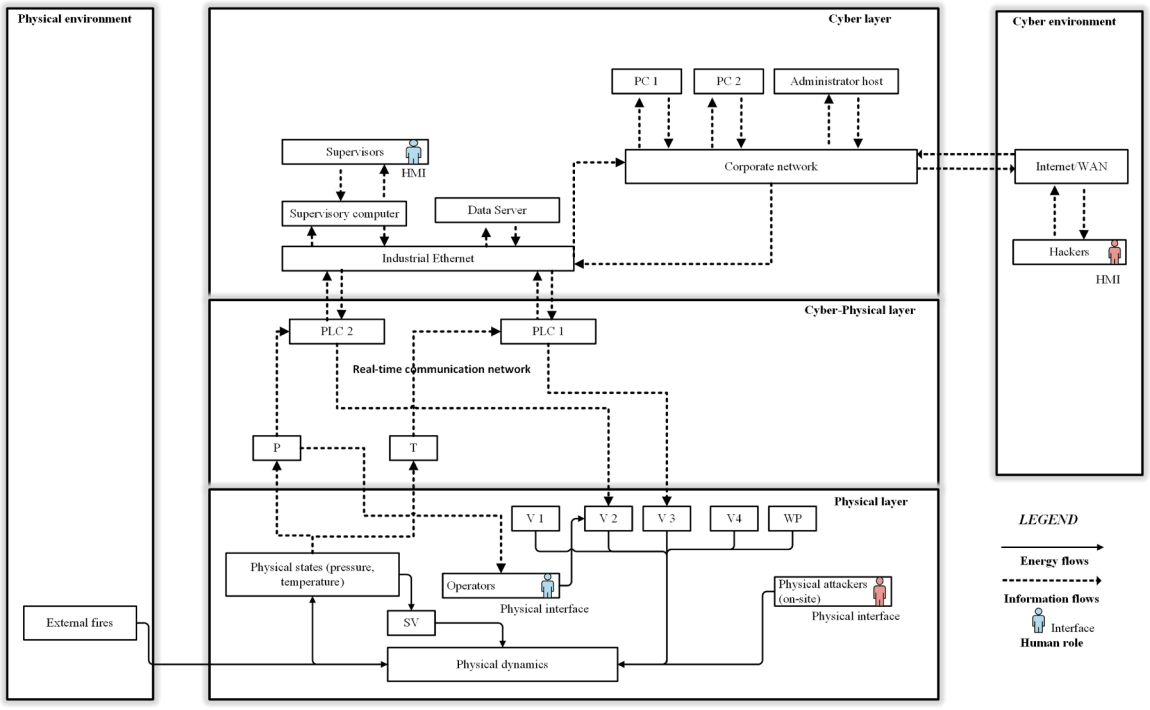


Fig. 7. CPS master diagram of the investigated chemical reactor.

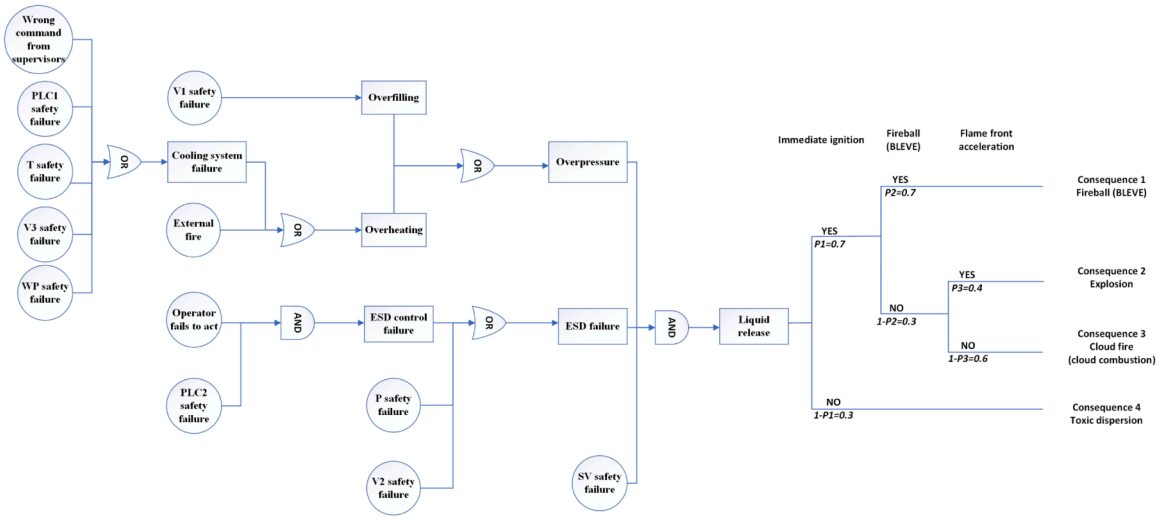


Fig. 8. Bow-tie diagram with a toxic and flammable liquid release as the central event, adapted from Vílchez et al. (2011).

(Andersen et al., 2004). Then, implementing a risk matrix helps visualize risk profiles considering both probabilities and consequence severities. The acceptance of risk may be decided by comparing the occurrence probability of each consequence to its threshold defined by experts or stakeholders.

Regarding sensitivity analysis, the ratio of variance (RoV) measure was introduced by Zarei et al. (2017) to identify critical root nodes of BN models. Both prior and posterior probabilities of the BN nodes are required in the calculation of RoV, as follows:

$$RoV_N = \frac{P^{'}(N) - P(N)}{P(N)} \tag{18}$$

where $P^{'}(N)$ is the posterior probability of node N and $P(N)$ is the prior probability of node N. By changing the state of the leaf/intermediate node (that denotes the undesired event) into "happening", the root node with a higher RoV value is more sensitive/critical. By using the RoV measure, the sensitivity of each root node to the happening of undesired events can be analyzed.

4. Case study: an application to a chemical reactor with its SCADA system

4.1. System representation and scenario building

In this case study, an integrated safety and security risk analysis of a continuous stirred tank reactor (CSTR) with its SCADA system is performed. This CSTR model runs a hypothetical exothermic first-order reaction A→B, and it is adapted from (Pilario and Cao, 2018). Product B is assumed to be a flammable liquid with toxicity. The CSTR with its SCADA system and safety instrumented system is shown in Fig. 6. A jacketed tank is deployed to maintain the temperature inside the reactor with industrial water provided by a water pump (WP). A control valve (V1) is implemented to feed reactant A at a fixed flow rate. Two PLCs are implemented to serve the automatic process control. PLC1 controls the coolant flow rate by regulating a control valve (V3) based on the measurement of a temperature sensor (T). PLC2 serves the emergency shutdown system (ESD) by activating the block/shutdown valve (V2) in case of overpressure is detected by the pressure sensor (P). A safety relief valve (SV) is installed to ensure the safety of the chemical reactor in case of overpressure. Both of the PLCs are supervised by site managers

Table 5
Identified threat agents and their corresponding attack modes.

Threat agents	Points-of-access (PoAs)	Attack targets or attack objectives	Attack modes	Is it capable to induce dangerous scenarios?	β coefficient in Eq. (14)	Marks
Hackers (with high-skill levels)	Device that is connected to external Internet/ WAN	Compromise PLC1 (cooling system) and PLC2 (ESD system), trigger dangerous overpressure scenarios	FDI attack against sensor T	YES	$\beta = 1$	AT1
			DoS attack against sensor T	YES	$\beta = 0.5$	AT2
			FDI attack against actuator V3	YES	$\beta = 1$	AT3
			DoS attack against actuator V3	NO	$\beta = 0$	/
			Setpoint manipulation of temperature threshold of PLC1	YES	$\beta = 1$	AT4
			FDI attack against sensor P	YES	$\beta = 1$	AT5
			DoS attack against sensor P	YES	$\beta = 1$	AT6
			FDI attack against actuator V2	YES	$\beta = 1$	AT7
			DoS attack against actuator V2	YES	$\beta = 1$	AT8
			Setpoint manipulation of overpressure threshold of PLC2	YES	$\beta = 1$	AT9
External physical attackers	Physical protection systems	Induce shell rupture and the release of hazardous chemicals	Physical attack with simple or major tools	YES	/	AT10

through the HMI (human-machine interface) of the SCADA system, which is linked to the corporate network and further the outside Internet/WAN. Considering the information flows and energy flows, a CPS master diagram of the chemical reactor is developed with the consideration of the human roles and the interactions between the CPS and external environments. The developed CPS master diagram is demonstrated in Fig. 7.

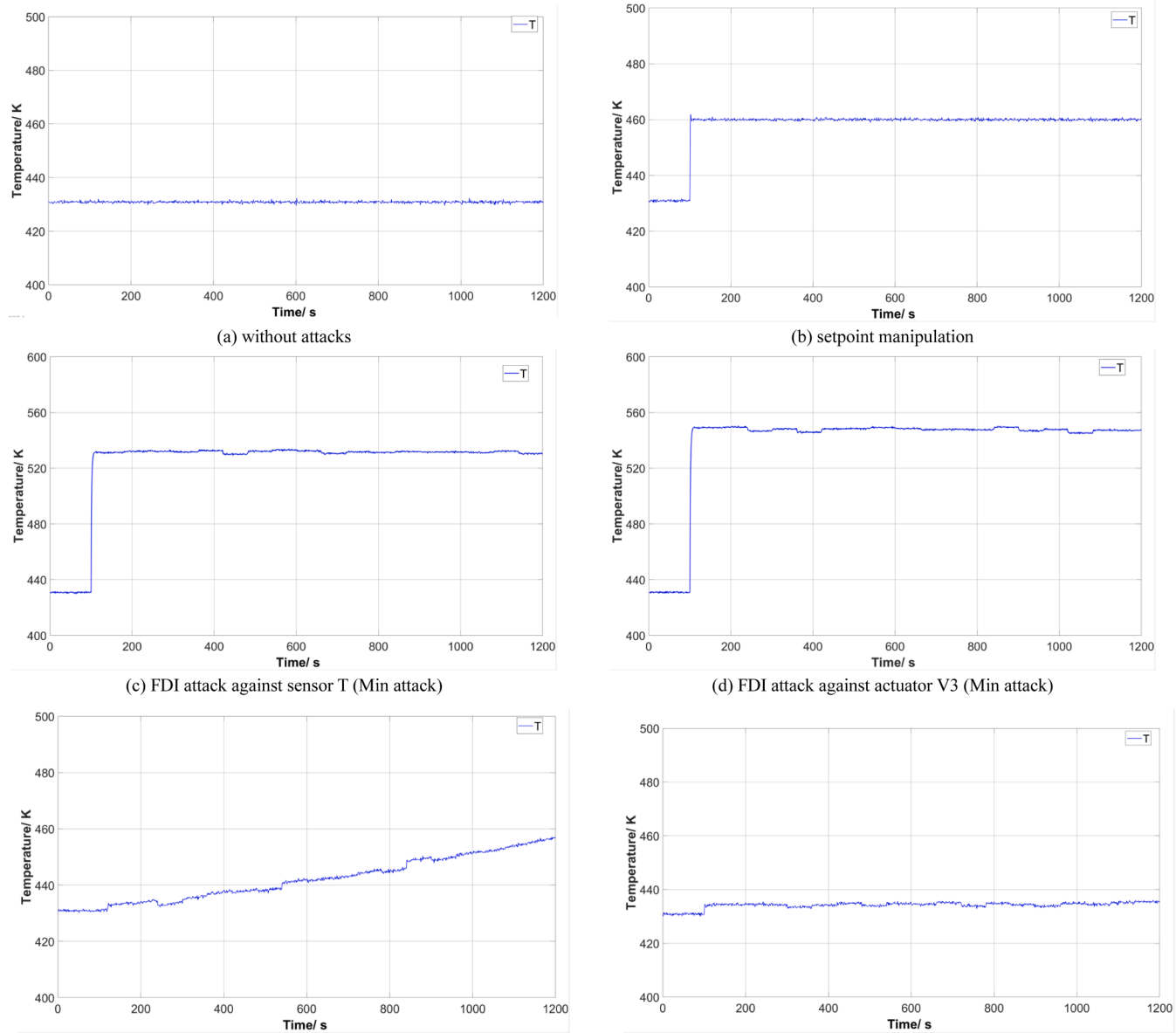
4.2. Risk assessment model development

4.2.1. Bow-tie diagram

Based on the CPS master diagram presented in Fig. 7, a bow-tie diagram for representing accident scenarios was constructed, as shown in Fig. 8. A release of toxic and flammable liquid was decided as the central event. Two safety barriers, which are an ESD system (emergency shutdown system) and a safety relief valve (SV), are deployed to prevent shell rupture in case of overpressure. At the left-hand side of the bow-tie diagram, a fault tree analysis was performed to identify the possible causes of a liquid release. At the right-hand side of the bow-tie diagram, a generic event tree for the release of toxic and flammable liquids adapted from Vílchez et al. (2011) is used.

4.2.2. Threat analysis and attack impact analysis

In this step, a threat analysis was performed first to identify threat agents and their corresponding PoAs (points of access), attack targets, and attack modes. From the conservative point of view, hackers with high-skill levels are identified as potential attackers implementing C2P attacks. Individuals or small groups driven by contingent intent with simple or major tools (TAC1) are identified as potential external physical attackers (SFK, 2002). According to the accident data analysis of security-related events in chemical plants (Landucci et al., 2020), terrorism mainly causes explosions as final scenarios, thefts and vandalisms are more likely to result in the release of hazardous chemicals, and C2P attacks mainly result in the loss of control of process systems. Therefore, the attack objectives of the physical attackers and hackers are identified as triggering the release of hazardous chemicals and



(a) without attacks

(b) setpoint manipulation

(c) FDI attack against sensor T (Min attack)

(d) FDI attack against actuator V3 (Min attack)

(e) DoS attack against sensor T (last received measurement is below the setpoint value)

(f) DoS attack against actuator V3

Fig. 9. Temperature inside the reactor under different C2P attack modes against the cooling system (attacks start from 100 s).

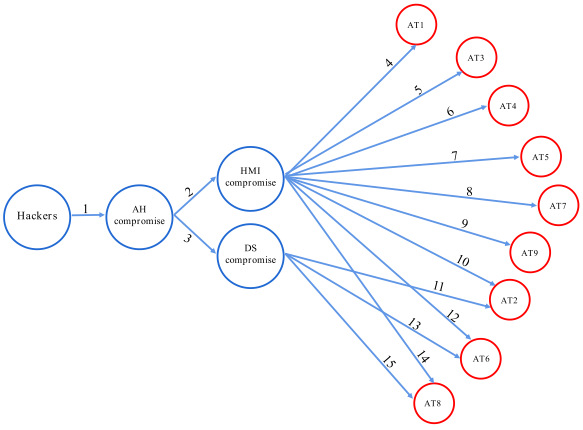


Fig. 10. Attack graph considering C2P attacks against the investigated industrial cyber-physical system with reference to Zhang et al. (2017) (explanations of AT1∼AT9 can be found in Table 5).

triggering the loss of control of the cooling system and ESD system, respectively. The obtained threat analysis results are given in Table 5.

For C2P attacks against PLC1, it is considered a dangerous overheating scenario when the temperature inside the reactor overpasses 450 K. Regarding Eq. (12), β coefficient can be calculated as $\beta = \Pr\{X(k) \notin R\} = \Pr\{T(k) > 450K\}$ ($X(k) = T(k)$ and $R = [-\infty, 450K]$). The physical impacts of different C2P attack modes were analyzed and the β coefficient for each attack mode was determined by implementing the approach presented in Section 3.4.3. Some selected results of the attack impact modeling are presented in Fig. 9. It was found that setpoint manipulations can induce overheating scenarios in a short time no matter the influence of process noise and observation noise, as shown in Fig. 9(b). Therefore, a successful setpoint manipulation has an extremely high likelihood of inducing a dangerous scenario (β=1). Similarly, FDI attacks (Min or Max Attacks) can induce overheating scenarios no matter the process noise and observation noise using the least attack time, as shown in Fig. 9(c) and (d). This finding is consistent with the results from Huang et al. (2009). By contrast, the DoS attacks cannot always induce overheating scenarios. Because the last received signal will be used under DoS attacks, the attack impact depends on both the attack duration and the last received signal before the attack. In this case study, both the measurement signal of sensor P and the control signal of actuator V3 follow normal distributions considering process noises and observation noises. By implementing a group of simulations, it was found that overheating can be induced by DoS attacks against sensor T only if the last received temperature signal is below the temperature setpoint (430.9 K), as shown in Fig. 9(e). The temperature measurement signal fluctuates around the setpoint and has a 50 % probability of being below the setpoint. Under the assumption that the attacker is able to perform an attack with an enough long duration, a successful DoS attack against sensor T has a 50 % probability of inducing a dangerous scenario (β=0.5). Regarding DoS attacks against actuator V3, it was found that overheating scenarios cannot be induced when the control signal of V3 is fluctuating within its operating range, as shown in Fig. 9(f). Therefore, β coefficient for DoS attacks against actuator V3 is 0 and this attack mode is not considered a dangerous attack mode.

In terms of C2P attacks against PLC2, all the attack modes are considered dangerous (β=1 for all attack modes against PLC2) because they are capable of making the ESD system fail to perform its functionality on demand no matter the process noise and observation noise. For instance, FDI attacks can inject malicious measurement data or control data to prevent the ESD system from being activated successfully on demand. DoS attacks can block the data flow and force the ESD system into an unactivated state. Setpoint manipulation of the overpressure threshold is capable of hindering the activation of shutdown actions even if the pressure already overpassed the pre-defined threshold. The determined β coefficient for each attack mode is summed up in Table 5. It should be noted that Table 5 doesn't provide a thorough list of security threats and the case study is only used for demonstration purposes. For instance, stealthy attacks and APTs (advanced persistent threats) are not considered in the case study. In practice, more security threats may exist, and it is possible to consider more security attack scenarios with credibility and perform an integrated safety and security risk assessment based on the proposed framework.

4.2.3. *Vulnerability analysis results*

In this study, the Adversary Sequence Diagrams and Path Analysis was employed to identify credible attack paths for physical attacks considering the deployment of physical protection systems (PPSs). The obtained site-specific adversary sequence diagram is shown in Fig. A1 in Appendix I. For simplicity, an event tree was used to perform a vulnerability assessment of PPSs, as shown in Fig. A2 in Appendix I. The PFDs (probability of failure on demand) of the PPSs were determined by using the approach and benchmark data introduced by Moreno et al. (2022).

In terms of the dangerous C2P attack modes, the information provided by the CPS master diagram helps to identify each attack step of the attacker. An ICS-specific vulnerability dataset (Thomas and Chothia, 2020) was used to identify the known vulnerabilities that may be exploited by the attacker at each attack step along the attack paths. Then, an attack graph was constructed to demonstrate the attack paths, as shown in Fig. 10. Local TTC (time-to-compromise) of each attack step is estimated using the approach presented in Appendix II, and the results are given in Table 6. The global TTC of each attack path was calculated by summing up the local TTCs of the attack steps along the attack path. For the attack modes with multiple attack paths, the shortest global TTC

Table 6
Time-to-compromise of each attack step.

Attack step number	Vulnerabilities (cve_id[a])	Average base score of CVSS v2.0	Average exploitability score of CVSS v3.0	TTC (days)	Attack step number	Vulnerabilities (cve_id)	Average base score of CVSS v2.0	Average exploitability score of CVSS v3.0	TTC (days)
1	CVE-2015–7871; CVE-2017–2683	9.00	3.35	5.28	2	CVE-2017–13997	9.80	3.90	5.94
3	CVE-2018–13799	9.10	3.90	5.94	4	no	/	/	40.01
5	no	/	/	40.01	6	CVE-2018–5459	9.80	3.90	5.64
7	no	/	/	40.01	8	no	/	/	40.01
9	CVE-2018–5459	9.80	3.90	5.64	10	CVE-2016–2200	7.50	3.90	5.99
11	CVE-2016–2200	7.50	3.90	5.99	12	CVE-2016–2200	7.50	3.90	5.99
13	CVE-2016–2200	7.50	3.90	5.99	14	CVE-2016–2200	7.50	3.90	5.99
15	CVE-2016–2200	7.50	3.90	5.99	/	/	/	/	/

[a] cve_id: A cve_id uniquely identifies one vulnerability from the Common Vulnerabilities and Exposures (CVE) database (NVD, N.d.).

Table 7
Estimation of shortest global time-to-compromise for each attack mode.

Attack mode	The shortest global TTC (days)	The conditional probability of successful attacks[a]	Attack mode	The shortest global TTC (days)	The conditional probability of successful attacks	Attack mode	The shortest global TTC (days)	The conditional probability of successful attacks
1	51.23	0.21	2	17.21	0.22	3	51.23	0.21
4	16.86	0.45	5	51.23	0.21	6	17.21	0.45
7	51.23	0.21	8	17.21	0.45	9	16.86	0.45

[a] The conditional probability of successful attacks for each attack mode is calculated using Eq. (14).

of each mode is used for security vulnerability quantification. Because all the dangerous C2P attack modes in the case study are assumed to be executed by remote attackers through network intrusions, network detection and response (NDR) is the main technology used to detect C2P attacks through the monitoring of network traffic (Pérez et al., 2021). A reference value (14 days) from Semertzis et al. (2022) is used as the MTTD value for all C2P attack modes in this case study. In practice, the MTTD value may be determined based on incident data analysis regarding specific intrusion types. The calculated shortest global TTC and the conditional probability of successful attacks (calculated by Eq. 14) for each attack mode are given in Table 7.

4.2.4. BN model development

For each attack mode in Table 5, a simplified attack tree was developed and attached to appropriate places in the bow-tie diagram. For instance, the attack tree for attack mode 1 (AT1 in Table 5) is composed of two basic events (the frequency of attempts to execute attack mode 1 and the conditional probability of the corresponding vulnerability being exploited successfully) and one top event (attack mode 1 is executed successfully). In this case study, all the attack trees were integrated into the left-hand-side of the bow-tie diagram (fault tree), as shown in Fig. 11. Then, a BN topology was developed based on the integrated attack-tree-bow-tie diagram, as shown in Fig. 12. All the BN nodes have two states (happening and not happening), except the consequences node, which is composed of five states (no consequence, fireball, explosion, cloud fire, and toxic dispersion). Table 8 gives prior probabilities of the root nodes. The abbreviations of other BN nodes are explained in Table 9.

4.3. Probabilistic risk assessment results

A Bayes net toolbox developed based on MATLAB (Murphy, 2001)

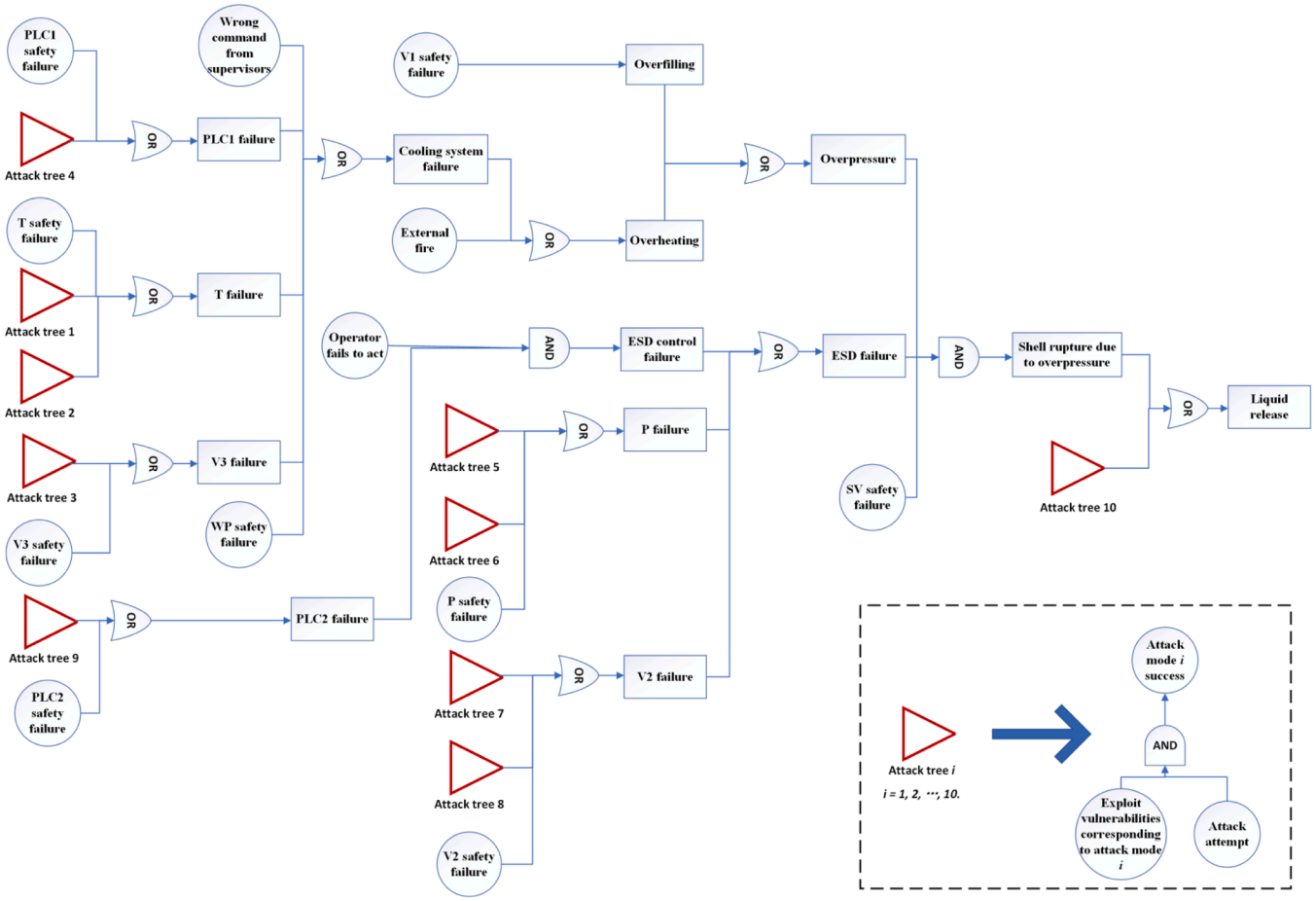


Fig. 11. The integration of the fault tree and attack trees.

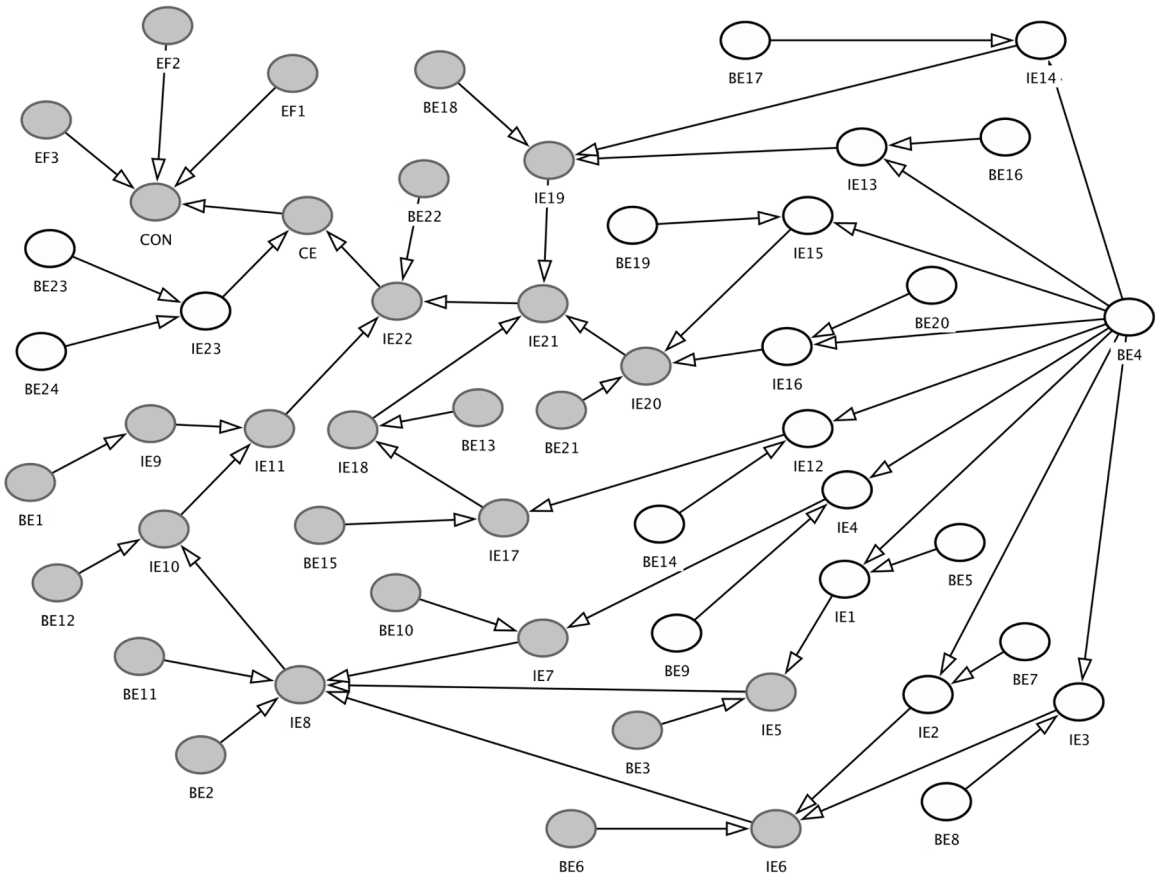


Fig. 12. Topology of the BN model (nodes without fillings are derived from attack trees and nodes with gray fillings are derived from the bow-tie diagram).

Table 8
Prior probabilities of the root nodes in the BN model.

Symbols	Root nodes	Prior probabilities	Sources	Symbols	Root nodes	Prior probabilities	Sources
BE1	V1 safety failure	4.00E-02	(Taylor, 2010)	BE2	Wrong command from supervisors	1.00E-01	(Andersen et al., 2004)
BE3	PLC1 safety failure	4.38E-02	(Hauge and Onshus, 2010)	BE4	C2P attack attempts	7.85E-01	Estimated withTable 3.
BE5	Exploit vulnerabilities corresponding to AT4	4.50E-01	Estimated by vulnerability assessment (Section 4.2.3)	BE6	T safety failure	2.13E-02	(Hauge and Onshus, 2010)
BE7	Exploit vulnerabilities corresponding to AT1	2.10E-01	Estimated by vulnerability assessment (Section 4.2.3)	BE8	Exploit vulnerabilities corresponding to AT2	2.20E-01	Estimated by vulnerability assessment (Section 4.2.3)
BE9	Exploit vulnerabilities corresponding to AT3	2.10E-01	Estimated by vulnerability assessment (Section 4.2.3)	BE10	V3 safety failure	4.00E-02	(Taylor, 2010)
BE11	WP safety failure	3.125E-02	(OREDA, 2002)	BE12	External fire	5.52E-02	(Debray et al., 2004)
BE13	Operator fails to shutdown	1.00E-02	(Andersen et al., 2004)	BE14	Exploit vulnerabilities corresponding to AT9	4.50E-01	Estimated by vulnerability assessment (Section 4.2.3)
BE15	PLC2 safety failure	1.00E-06	(Hauge and Onshus, 2010)	BE16	Exploit vulnerabilities corresponding to AT5	2.10E-01	Estimated by vulnerability assessment (Section 4.2.3)
BE17	Exploit vulnerabilities corresponding to AT6	4.50E-01	Estimated by vulnerability assessment (Section 4.2.3)	BE18	P safety failure	1.50E-07	(Hauge and Onshus, 2010)
BE19	Exploit vulnerabilities corresponding to AT7	2.10E-01	Estimated by vulnerability assessment (Section 4.2.3)	BE20	Exploit vulnerabilities corresponding to AT8	4.50E-01	Estimated by vulnerability assessment (Section 4.2.3)
BE21	V2 safety failure	3.50E-06	(Hauge and Onshus, 2010)	BE22	SV safety failure	2.40E-03	(Hauge and Onshus, 2010)
BE23	External physical attacks	3.30E-02	Estimated withTable 2 (1/Λ, Λ=30 years).	BE24	Exploit vulnerabilities of PPSs	4.20E-01	Estimated by vulnerability assessment (Appendix I)
EF1	Immediate ignition	7.00E-01	(Vílchez et al., 2011)	EF2	Fireball (BLEVE)	7.00E-01	(Vílchez et al., 2011)
EF3	Flame front acceleration	4.00E-01	(Vílchez et al., 2011)	/	/	/	/

was used to perform the risk assessment by using the prior probabilities presented in Table 8. Additionally, the risks purely caused by safety causes are assessed by configuring the prior probabilities of security attacks into zeros. We used a risk matrix to visualize the major accident risks induced by safety hazards and the combination of safety hazards and security threats, as shown in Fig. 13. It is observed that the risks of safety-associated major accidents (fireball, explosion, cloud fire, and toxic dispersion) are all within the green region, which means the safety risks are acceptable. However, the major accident risks estimated by integrating safety-associated scenarios and security-related attack

Table 9
Explanations of the leaf node and intermediate nodes.

Symbols	Node names	Symbols	Node names	Symbols	Node names	Symbols	Node names
IE1	AT4 success	IE2	AT1 success	IE3	AT2 success	IE4	AT3 success
IE5	PLC1 failure	IE6	T failure	IE7	V3 failure	IE8	Cooling system failure
IE9	Overfilling	IE10	Overheating	IE11	Overpressure	IE12	AT9 success
IE13	AT5 success	IE14	AT6 success	IE15	AT7 success	IE16	AT8 success
IE17	PLC2 failure	IE18	ESD control failure	IE19	P failure	IE20	V2 failure
IE21	ESD failure	IE22	Shell rupture due to overpressure	IE23	AT10 success	CE	Liquid release
CON	Consequences	/	/	/	/	/	/

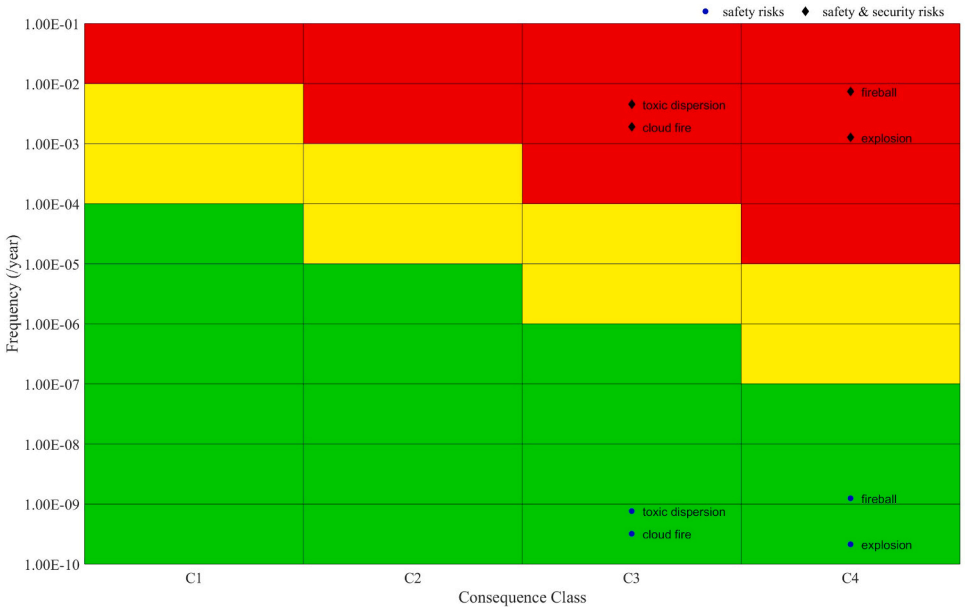


Fig. 13. A risk matrix presenting major accident risks induced by safety hazards and the combination of safety hazards and security threats.

scenarios become unacceptable and are much higher than the pure-safety risks. The estimated annual frequencies of the occurrence of major accidents (fireball, explosion, cloud fire, and toxic dispersion) considering both safety hazards and security threats are between 10^{-3} to 10^{-2}. This result indicates that it is necessary to integrate security attack scenarios into the safety risk assessment of ICPSs, otherwise, major accident risks may be underestimated.

5. Discussion

5.1. Sensitivity analysis of root nodes

To identify critical causes leading to major accidents, this section uses the RoV measure to perform a sensitivity analysis of the basic events (root nodes). Concerning the occurrence of major accidents (fireball, explosion, cloud fire, and toxic dispersion), the RoV value of each root node is calculated using Eq. (18). The calculated RoV values of the safety-associated basic events and security-associated basic events are presented in Fig. 14 (a) and (b) respectively. Fig. 14 (a) shows that BE22 (SV safety failure) has a sensitivity significantly ahead of others, followed by BE18 (P safety failure) and BE21 (V2 safety failure). Those three events are related to the failure of safety barriers (emergency shutdown system and safety relief valve), which means safety barriers play important roles in preventing major accidents. Particularly, as a passive safety barrier, the safety relief valve (SV) is the most critical equipment. BE15 (PLC2 safety failure) has the smallest sensitivity, and it is followed by BE13 (Operator fails to shutdown). Because BE15 and BE13 take the same responsibility to activate the shutdown valve (V2) based on the received measurement signals from pressure sensor (P), they may reduce each other's criticality/sensitivity to certain extents. The remaining safety-associated basic events (BE1, BE2, BE3, BE6, BE10, BE11, and BE12) have nearly the same sensitivity, which means they have similar importance.

Regarding security-associated basic events, BE23 (External physical attacks) and BE24 (Exploit vulnerabilities of PPSs) have dominant sensitivities. It means that physical attack is the most threatening attack mode and the vulnerability subject to the physical attack is the most critical security vulnerability. One reason for this result is that physical attacks can overpass the protection of some safety barriers (ESD system and safety relief valve in this study) and induce the loss of contaminant through damaging equipment directly. Regarding C2P attacks, BE14 (Exploit vulnerabilities corresponding to AT9) has the smallest sensitivity, while BE5, BE7, BE8, BE9, BE16, BE17, BE19, and BE20 have almost the same sensitivity. This result demonstrates that the vulnerabilities subject to each C2P attack mode have similar sensitivities, except the vulnerabilities subject to AT9 (setpoint manipulation of the overpressure threshold of PLC2). The reason may be that manual emergency shutdown in case of PLC2 failures reduces the danger of cyberattacks against PLC2. The sensitivity analysis results indicate the importance of protecting digitalized safety barriers from cyberattacks and the necessity of deploying physical/passive barriers and human barriers to prevent major accidents.

5.2. Influence of security-associated parameters on major accident risks

Because some conservative or rough assumptions were made to some parameters in the security analysis, for instance, hackers were assumed to be with high-skill levels and rough reference values were used for

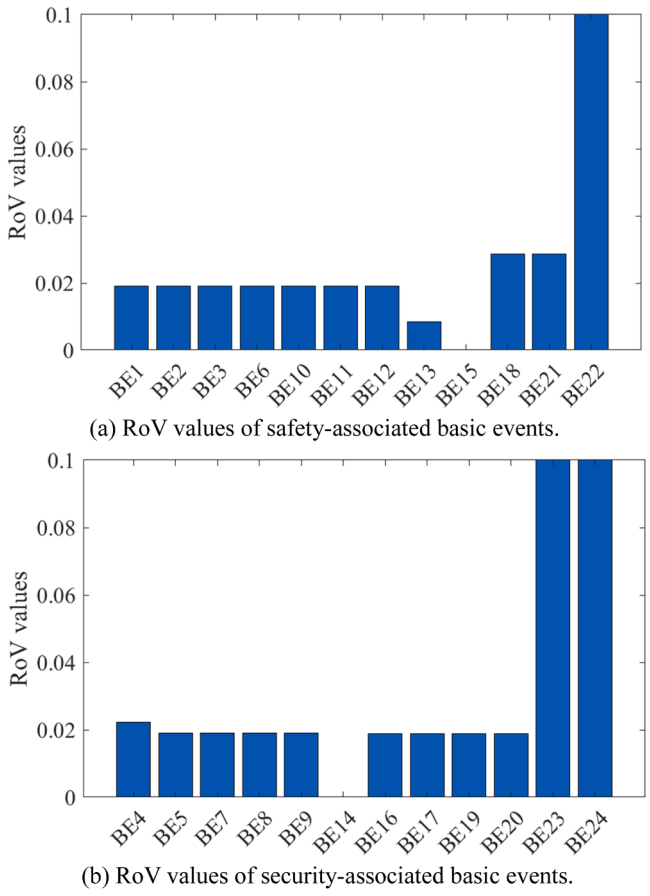


Fig. 14. Sensitivity analysis of BN root nodes.

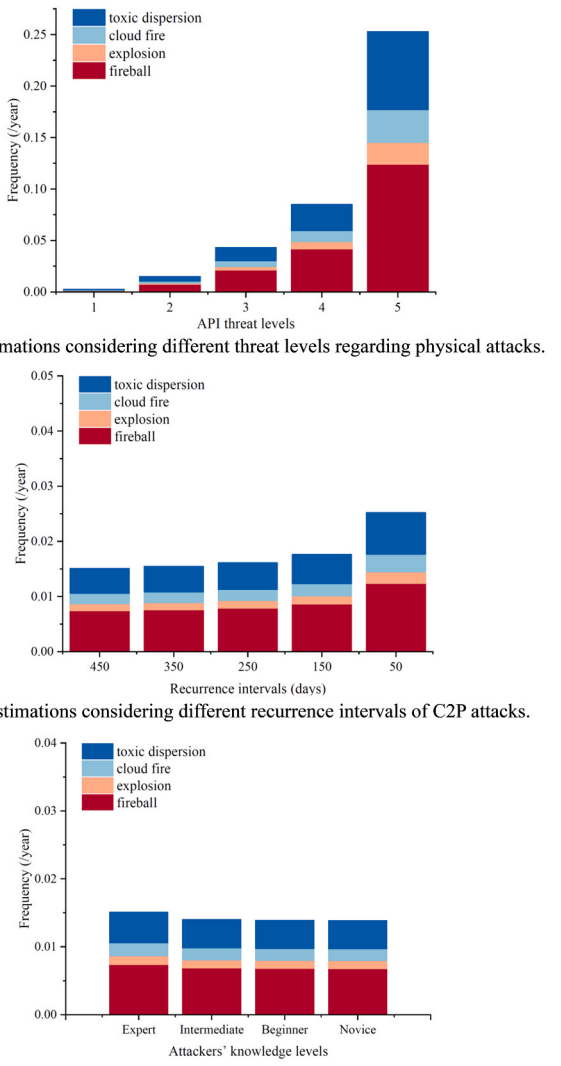


Fig. 15. A comparison of risk assessment results under different configurations of security-associated parameters.

annual probabilities of C2P attacks and physical attacks, it is essential to get indications on how the uncertainty associated with those parameters may influence the risk assessment results. Therefore, major accident risks obtained by configuring different setups/values to those parameters are compared and presented in Fig. 15. As shown in Fig. 15 (a), major accident risks estimated by using different API threat levels for external physical attacks are demonstrated in the form of a stacked column chart. With the threat level varying from 1 to 5 (attack annual probability varying from 3.3E-03–6.0E-01), the annual probability of happening of major accidents increases significantly, from 2.6E-03–2.5E-01. This result is consistent with the sensitivity analysis results presented in Section 5.1, which reflects that the major accident risks are highly sensitive to the annual probability of physical attacks. Similarly, major accident risks estimated by using different recurrence intervals and different attackers' knowledge levels for C2P attacks are compared in Fig. 15 (b) and (c) respectively. The results show that major accident risks are sensitive to the recurrence interval of C2P attacks. With the recurrence interval of C2P attacks varying from 450 days to 50 days, the annual probability of happening of major accidents increases from 1.5E-02–2.5E-02. By contrast, major accident risks are less sensitive to the attackers' knowledge levels. With the attackers' knowledge levels varying from expert to novice, the annual probability of happening of major accidents reduces from 1.5E-02–1.4E-02.

6. Conclusions

This study proposes an approach for integrated safety and security risk analysis of industrial cyber-physical systems (ICPSs) with respect to major accident scenarios in chemical plants. The proposed approach helps to perform a comprehensive risk analysis of ICPSs considering safety hazards, security threats, and the interdependency between safety-associated and security-related adverse events. A case study was used to demonstrate the integration of potential physical attack and C2P attack scenarios into the safety risk analysis of a chemical reactor. According to the risk assessment results, major safety-related accident risks may increase to a large extent with the involvement of potential security attack scenarios. The assessment of only safety-associated scenarios or security attack scenarios may lead to a risk underestimation. A sensitivity analysis was performed to identify critical safety-associated and security-associated basic events. The results indicate that the vulnerabilities of ICPSs to cyberattacks should be given enough attention, particularly considering the possible C2P attacks on digitalized safety barriers. Moreover, it is found that physical/passive barriers and human barriers play an important role in preventing the happening of disastrous consequences. Because physical/passive barriers and human barriers are not subjected to cyberattacks, they can be considered critical measures to prevent the occurrence of C2P attack-induced disastrous scenarios.

Although the demonstrated case study focuses on the safety and security of chemical facilities, it is also possible to apply the proposed approach with modifications to quantitative risk analysis of ICPSs in other sectors. This can be done by applying the overall framework of the approach and with the adaptation of some tools (for instance, CPS master diagram, bow-tie, and attack/compromise graph) considering the specific information and operation features of the investigated ICPS

and the possible dangerous scenarios. Because ICPSs in other sectors may have different safety operating mechanisms and attack defense/response mechanisms, the application of the proposed approach to risk assessment of ICPSs in other sectors may be investigated in future studies. Due to the lack of data, attack likelihood estimation regarding both physical attacks and C2P attacks is tricky in practice. Although some reference data in the chemical process industries or other similar sectors is helpful, the estimation of attack likelihood may be still highly subjective. Additionally, some conservative assumptions were made in the vulnerability analysis, for instance, the shortest global TTC is used with the ignorance of attackers' intrusion path selection and attackers are assumed with high knowledge levels. The uncertainties associated with the rough or conservative assumptions in threat analysis and vulnerability analysis need to be evaluated and properly handled in future studies.

CRediT authorship contribution statement

Shuaiqi Yuan: Methodology, Conceptualization, Visualization, Investigation, Writing – original draft. **Ming Yang:** Formal analysis, Supervision, Writing – review & editing. **Genserik Reniers:** Supervision, Conceptualization, Writing – review & editing.

Declaration of Competing Interest

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

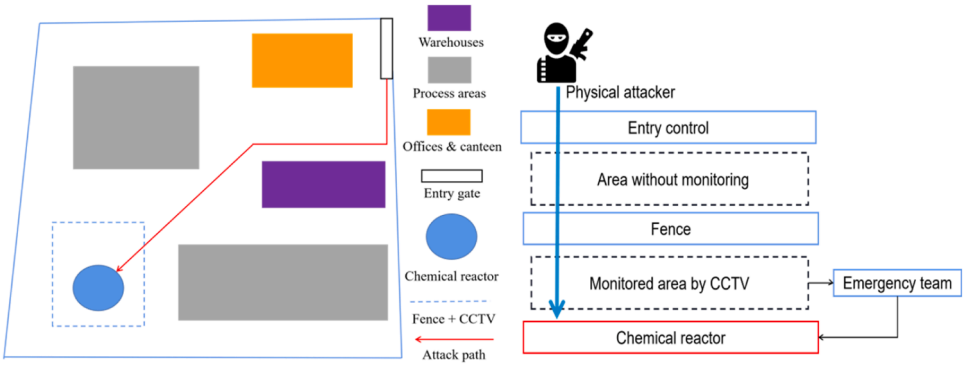
Data availability

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

Acknowledgements

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

Appendix I



(a) Layout of the chemical plant. (b) Adversary sequence diagram.

Fig. A1. Site-specific adversary sequence diagram considering external physical attacks.

.

Four types of PPSs are considered in this study and the benchmark data are derived from Moreno et al. (2022), as presented in Table A1. AIT (adversary intrusion time) and ERT (emergency response time) are employed to evaluate the effectiveness of the emergency team. In the investigated case study, it is assumed that when the fence works for delaying the attackers effectively, AIT > ERT. Otherwise, AIT < ERT and the emergency team cannot prevent the attack effectively. According to Fig. A2, the conditional probability of a successful physical attack given an attack attempt is calculated as: $P_s = P_1 + P_2 + P_4 + P_5 = 0.42$.

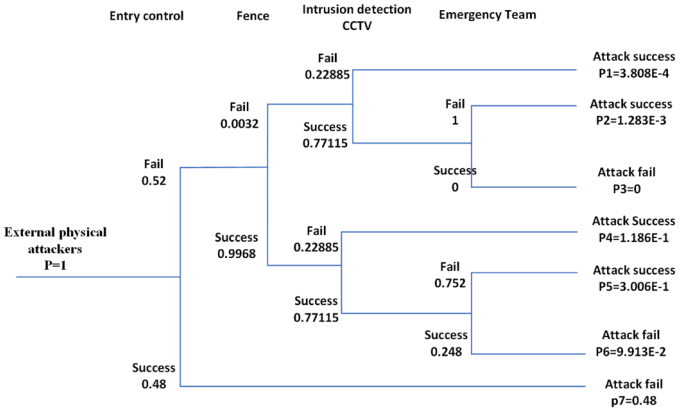


Fig. A2. Event tree analysis of the external physical attack.

Table A1
Fail probabilities and success probabilities of PPSs, adapted from Moreno et al. (2022).

PPS (physical protection system)	PFD (probability of failure on demand)	Effectiveness (η)	Calculation formulas
Entry control	0.40	0.80	$P_{fail} = PFD + (1-\eta) \times (1-PFD)$
Fence	0.00	0.9968	$P_{success} = (1-PFD) \times \eta$
Closed Circuit TeleVision (CCTV)	0.205	0.97	
Emergency Team	0.752	1 if AIT > ERT; 0 if AIT < ERT	$P_{success} = (1-PFD) \times \eta$ $P_{fail} = 1-(1-PFD) \times \eta$

Appendix II

In the TTC estimation approach, TTC is modeled as a random process composed of three subprocesses: i) at least one vulnerability is known, and the attacker has the exploit readily available that can be used to exploit the known vulnerability successfully, ii) at least one vulnerability is known, but the attacker must develop an exploit for it, and iii) the attacker must find and exploit new vulnerabilities because either no known vulnerabilities exist or the attacker is unable to exploit known vulnerabilities. The expected TTC of an attack step is estimated as follows (McQueen et al., 2006; Ling and Ekstedt, 2022).

$$TTC = t_1 P_1 + t_2(1-P_1)(1-u) + t_3 u(1-P_1) \tag{A1}$$

where t_i is the expected time used in subprocess i (i= *1, 2, 3*) in days and P_1 is the probability of being in subprocess 1. u is the probability that subprocess 2 is unsuccessful. The probabilities for an attacker to be in subprocess 1 and 2 are calculated as follows (Ling and Ekstedt, 2022).

$$P_1 = 1 - e^{-vm/k} \tag{A2}$$

$$P_2 = e^{-vm/k} = 1 - P_1 \tag{A3}$$

where v is the number of vulnerabilities on a specific component and m is the number of exploits readily available to the attacker. k is the total number of vulnerabilities in the database. The value of k is 2740 according to the ICS vulnerability dataset (Thomas and Chothia, 2020) available on October 5th, 2023. Subprocess 3 is considered running in parallel to subprocess 1 and 2, therefore, there is no need to estimate the probability of an attacker to be in subprocess 3. The time taken to complete each subprocess is estimated as below (Ling and Ekstedt, 2022).

$$t_1 = 1 * ((10/C_2 + 3.9/C_3)2) \tag{A4}$$

$$t_2 = 37\ (\text{novice}), 27\ (\text{beginner}),\ 16\ (\text{intermediate}),\ \text{or}\ 6\ (\text{expert}) \tag{A5}$$

$$t_3 = (f^{'} - 0.5) * b + t_2 \tag{A6}$$

where C_2 is the average base score of the vulnerabilities derived from CVSS v2.0[1] and C_3 is the average exploitability score of the vulnerabilities derived from CVSS v3.0.[2] In terms of t_2, 37 days, 27 days, 16 days, and 6 days are used for novice, beginner, intermediate, and expert attackers respectively. b is the MeanTime-Between-Vulnerabilities (MTBV) in days as calculated from the ICS advisory creation date (Thomas and Chothia, 2020). f is the fraction of vulnerabilities that are exploitable to the attacker, and it is determined based on Table A2. The probability that subprocess 2 is unsuccessful (u) is calculated as $u = (1-f)^v$. An Excel tool[3] developed by Thomas and Chothia (2020) was used to perform the TTC estimations.

Table A2
The number and fraction of exploitable vulnerabilities to attackers with different skill levels, adapted from Ling and Ekstedt (2022).

Skill level	CVSS exploitability range	Exploitable vulnerabilities	Fraction of exploitable vulnerabilities
Expert	0.1–3.9	1916	1
Intermediate	0.1–3	966	0.50
Beginner	0.1–2.1	455	0.24
Novice	0.1–1.2	105	0.05

[1] CVSS v2.0 user guide. (n.d.). Retrieved October 06, 2023, from https://www.first.org/cvss/v2/guide.
[2] CVSS v2.0 user guide. (n.d.). Retrieved October 06, 2023, from https://www.first.org/cvss/v3.0/user-guide.
[3] TTC-ICS. Retrieved October 06, 2023, from https://github.com/EngLi/ttc-ics.

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.

Alanen, J., Linnosmaa, J., Malm, T., Papakonstantinou, N., Ahonen, T., Heikkilä, E., Tiusanen, R., 2022. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. Reliab. Eng. Syst. Saf. 220, 108270.

American Petroleum Institute (API), 2013. ANSI/API standard 780 – security risk assessment methodology for the petroleum and petrochemical industry. American Petroleum Institute, Washington, DC.

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.

Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliab. Eng. Syst. Saf. 71 (*3*), 249–260.

Cárdenas, A.A., Amin, S., Lin, Z.S., Huang, Y.L., Huang, C.Y., Sastry, S., 2011, March. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the Sixth ACM Symposium on Information, Computer and Communications Security, 355–366.

Casciano, M., Khakzad, N., Reniers, G., Cozzani, V., 2019. Ranking chemical industrial clusters with respect to safety and security using analytic network process. Process Saf. Environ. Prot. 132, 200–213.

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

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.

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. École Nationale Supérieure de Mines de Saint Etienne, France, p. 100.

Flaus, J.M., 2019. Cybersecurity of Industrial Systems. John Wiley & Sons.

Freeman, R.A., 1990. CCPS guidelines for chemical process quantitative risk analysis. Plant/Oper. Prog. 9 (*4*), 231–235.

Friedberg, I., McLaughlin, K., Smith, P., Laverty, D., Sezer, S., 2017. STPA-SafeSec: safety and security analysis for cyber-physical systems. J. Inf. Secur. Appl. 34, 183–196.

George, P.G., Renjith, V.R., 2021. Evolution of safety and security risk assessment methodologies towards the use of bayesian networks in process industries. Process Saf. Environ. Prot. 149, 758–775.

Gribaudo, M., Iacono, M., Marrone, S., 2015. Exploiting Bayesian networks for the analysis of combined attack trees. Electron. Notes Theor. Comput. Sci. 310, 91–111.

Guzman, N.H.C., Wied, M., Kozine, I., Lundteigen, M.A., 2020. Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. Syst. Eng. 23 (*2*), 189–210.

Hauge, S., Onshus, T. , 2010. Reliability Data for Safety Instrumented Systems PDS Data Handbook, 2010 ed.. SINTEF Report A, 13502.

Henry, M.H., Haimes, Y.Y., 2009. A comprehensive network security risk model for process control networks. Risk Anal. Int. J. 29 (*2*), 223–248.

Hu, Y., Li, H., Yang, H., Sun, Y., Sun, L., Wang, Z., 2019. Detecting stealthy attacks against industrial control systems based on residual skewness analysis. EURASIP J. Wirel. Commun. Netw. 2019 (1), 1–14.

Huang, K., Zhou, C., Tian, Y.C., Yang, S., Qin, Y., 2018. Assessing the physical impact of cyberattacks on industrial cyber-physical systems. IEEE Trans. Ind. Electron. 65 (10), 8153–8162.

Huang, Y.L., Cárdenas, A.A., Amin, S., Lin, Z.S., Tsai, H.Y., Sastry, S., 2009. Understanding the physical and economic consequences of attacks on control systems. Int. J. Crit. Infrastruct. Prot. 2 (*3*), 73–83.

IEC, 2020. 62443-3-2: Security for Industrial Automation and Control Systems–Part 3-2: Security Risk Assessment For System Design. International Electrotechnical Commission, Geneva.

Jensen, F.V., Nielsen, T.D., 2007. Bayesian Networks And Decision Graphs, 2. Springer, New York.

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.

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.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y., 2015. A survey of approaches combining safety and security for industrial control systems. Reliab. Eng. Syst. Saf. 139, 156–178.

Kuypers, M., Maillart, T. , 2018, June. Designing organizations for cyber security resilience. In: Proceedings of the 2018 The Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria, 18–19.

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., Khakzad, N., Reniers, G., 2020. Physical Security In The Process Industry: Theory with Applications. Elsevier.

Ling, E.R., Ekstedt, M., 2022. Estimating the Time-To-Compromise of Exploiting Industrial Control System Vulnerabilities. ICISSP 96–107.

Ling, E.R., Ekstedt, M., 2023. Estimating time-to-compromise for industrial control system attack techniques through vulnerability data. SN Comput. Sci. 4 (*3*), 318.

McQueen, M.A., Boyer, W.F., Flynn, M.A., Beitel, G.A., 2006. Time-to-compromise model for cyber risk reduction estimation. In: Quality of Protection: Security Measurements and Metrics. Springer, US, pp. 49–64.

Meyer, T., Reniers, G., 2022. Engineering Risk Management. Walter de Gruyter GmbH & Co KG.

Moreno, V.C., Marroni, G., Landucci, G., 2022. Probabilistic assessment aimed at the evaluation of escalating scenarios in process facilities combining safety and security barriers. Reliab. Eng. Syst. Saf. 228, 108762.

Mughal, A.A., 2022. Building and securing the modern security operations center (SOC). Int. J. Bus. Intell. Big Data Anal. 5 (*1*), 1–15.

Murphy, K., 2001. The bayes net toolbox for matlab. Comput. Sci. Stat. 33 (*2*), 1024–1034.

National Vulnerability Database (NVD). (n.d.). Retrieved February 24, 2023, from https://nvd.nist.gov/.

Norman, T.L., 2010. Risk Analysis And Security Countermeasure Selection. CRC Press, Boca Raton/London/New York.

OREDA, 2002. Offshore Reliability Data Handbook. DNV, Trondheim, Norway.

Orojloo, H., Azgomi, M.A., 2017. A game-theoretic approach to model and quantify the security of cyber-physical systems. Comput. Ind. 88, 44–57.

Pérez, S.I., Moral-Rubio, S., Criado, R., 2021. A new approach to combine multiplex networks and time series attributes: building intrusion detection systems (IDS) in cybersecurity. Chaos Solitons Fractals 150, 111143.

Pilario, K.E.S., Cao, Y., 2018. Canonical variate dissimilarity analysis for process incipient fault detection. IEEE Trans. Ind. Inform. 14 (12), 5308–5315.

Reniers, G., Khakzad, N., 2017. Revolutionizing safety and security in the chemical and process industry: applying the CHESS concept. J. Integr. Secur. Saf. Sci. 1 (*1*), 2–15.

Reniers, G., Khakzad, N., van Gelder, P., 2017. Security Risk Assessment In the Chemical and Process Industry. (Integrated Security Science). Walter de Gruyter. ⟨https://www.degruyter.com/viewbooktoc/product/477259⟩.

Semertzis, I., Rajkumar, V.S., Ştefanov, A., Fransen, F., Palensky, P., 2022. Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs. In: Proceedings of the Tenth Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES). IEEE, pp. 1–6. In 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES).

Störfall Kommission (SFK), 2002. SFK-GS-38 Report.

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 March 2023).

Thomas, R.J., Chothia, T., 2020. Learning from vulnerabilities - categorising, understanding and detecting weaknesses in industrial control systems. In: Computer Security. Springer International Publishing, Cham.

Tong, X., Fang, W., Yuan, S., Ma, J., Bai, Y., 2018. Application of Bayesian approach to the assessment of mine gas explosion. J. Loss Prev. Process Ind. 54, 238–245.

Vílchez, J.A., Espejo, V., Casal, J., 2011. Generic event trees and probabilities for the release of different types of hazardous materials. J. Loss Prev. Process Ind. 24 (*3*), 281–287.

Wen, H., Khan, F., Ahmed, S., Imtiaz, S., Pistikopoulos, S., 2023. Risk assessment of human-automation conflict under cyberattacks in process systems. Comput. Chem. Eng. 172, 108175.

Yampolskiy, M., Horvath, P., Koutsoukos, X.D., Xue, Y., Sztipanovits, J. , 2013, April. Taxonomy for description of cross-domain attacks on CPS. In: Proceedings of the Second ACM International Conference On High Confidence Networked Systems, 135–142.

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., Reniers, G., Yang, M., 2023b. Dynamic-risk-informed safety barrier management: an application to cost-effective barrier optimization based on data from multiple sources. J. Loss Prev. Process Ind. 83, 105034.

Yuan, S., Reniers, G., Yang, M., Bai, Y., 2023a. Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm. Process Saf. Environ. Prot. 170, 356–371.

Yuan, S., Yang, M., Reniers, G., Chen, C., Wu, J., 2022. Safety barriers in the chemical process industries: a state-of-the-art review on their classification, assessment, and management. Saf. Sci. 148, 105647.

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.

Zhang, Q., Zhou, C., Tian, Y.C., Xiong, N., Qin, Y., Hu, B., 2017. A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. IEEE Trans. Ind. Inform. 14 (6), 2497–2506.

Zhang, Y., Wang, L., Xiang, Y., Ten, C.W., 2015. Power system reliability evaluation with SCADA cybersecurity considerations. IEEE Trans. Smart Grid 6 (4), 1707–1721.