Risk assessment methods for process safety, process security and resilience in the chemical process industry

A thorough literature review

Bin Ab Rahim, M.S.; Reniers, Genserik; Yang, Ming; Bajpai, Shailendra

DOI
10.1016/j.jlp.2024.105274

Publication date
2024

Document Version
Final published version

Published in
Journal of Loss Prevention in the Process Industries

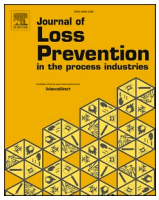
Citation (APA)
Bin Ab Rahim, M. S., Reniers, G., Yang, M., & Bajpai, S. (2024). Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review. *Journal of Loss Prevention in the Process Industries*, *88*, Article 105274. https://doi.org/10.1016/j.jlp.2024.105274

Journal of Loss Prevention in the Process Industries 88 (2024) 105274

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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



Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review

Muhammad Shah Ab Rahim [a,b,*], Genserik Reniers [a,c,d], Ming Yang [a,e,f], Shailendra Bajpai [g]

[a] Safety and Security Science Section, Faculty of Technology, Policy and Management, TU Delft, 2628 BX Delft, the Netherlands
[b] Department of Occupational Safety and Health Malaysia, Ministry of Human Resources, Government Administrative Centre, Putrajaya 62530, Malaysia
[c] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000 Antwerp, Belgium
[d] CEDON, KU Leuven, 1000 Brussels, Belgium
[e] Centre of Hydrogen Energy, Institute of Future Energy, Universiti Teknologi Malaysia, 81310 UTM Johor Bahru, Johor, Malaysia
[f] National Centre of Maritime Engineering and Hydrodynamics Australia Maritime College, University of Tasmania, Launceston, Tasmania, Australia
[g] Department of Chemical Engineering, Dr B.R. Ambedkar National Institute of Technology, Jalandhar, Punjab, India

ARTICLE INFO

Keywords:
Chemical process industry
Process safety
Process security
Resilience
Risk assessment
Sociotechnical systems

ABSTRACT

This paper presents a systematic literature review of risk assessment methods in the chemical process industry (CPI), focusing on process safety, process security, and resilience. We analyzed peer-reviewed articles from 2000 to 2022 using the PRISMA methodology and identified twelve predominant methods. Our findings reveal a shift towards dynamic, systemic-based assessments like the Functional Resonance Analysis Method (FRAM) and System-Theoretic Accident Model and Processes (STAMP). These methods are particularly effective at capturing the complexities of sociotechnical systems in the CPI. However, a significant observation from our review is the limited emphasis on the resilience paradigm within many existing methods when addressing both process safety and process security risks, which is crucial for preventing and recovering from disruptions. Given the evolving challenges in system safety and security threats, there is an urgent need for holistic methods that integrate process safety, process security, and resilience. Our review highlights the opportunity for further research to better prepare the industry for future challenges, ensuring safer, more secure, reliable, and resilient operations.

1. Introduction

1.1. Context

The chemical process industry (CPI) are an essential component of the global economy, with worldwide revenue stood at some 4.73 trillion U.S. dollars in 2021 (American Chemistry Council, 2022), and responsible for producing a wide range of products and materials vital to various sectors, such as pharmaceuticals, agriculture, and consumer goods. However, the complex nature of CPI operations and the presence of hazardous materials and equipment expose these industries and their surroundings to significant process safety concerns, such as fire and explosions, unintentional toxic releases, and acute and chronic effects on humans and the environment (Amin et al., 2022). Besides process safety risks, process security risks also have emerged as key concerns for organizations operating in the CPI sector, as evidenced by 373 security-related incidents throughout history (Iaiani et al., 2021).

Although the majority of workplace accidents are caused by type I risks, which are occupational accidents (such as falls and small fires) and minor security events (such as petty theft), type II risks, which are major accidents or incidents can result in a catastrophic event, also frequently occur with numerous fatalities and major asset damages. To help readers better grasp the focus of this paper on type II risk, we have laid out the differences in risk types between safety and security in Table 1.

Actually, from a global viewpoint, type II incidents happen semi-regularly, including major fires, explosions, and large toxic releases (Meyer and Reniers, 2022). Notable process safety-related accidents include the Flixborough disaster (1974), the Bhopal gas tragedy (1984), the Texas City refinery explosion (2005), and the Deepwater Horizon catastrophe (2010), which were caused by safety-related factors such as inadequate safety measures, insufficient training, and/or poor maintenance (Amyotte et al., 2016; Kleindorfer et al., 2012). These incidents highlight the importance of robust process safety risks assessment methodologies, such as Hazard and Operability Study (HAZOP), Layer of

* Corresponding author. Safety and Security Science Section, Faculty of Technology, Policy and Management, TU Delft, 2628 BX Delft, the Netherlands.
E-mail address: mdshah@mohr.gov.my (M.S. Ab Rahim).

https://doi.org/10.1016/j.jlp.2024.105274
Received 23 October 2023; Received in revised form 22 January 2024; Accepted 11 February 2024
Available online 19 February 2024

Protection Analysis (LOPA), and Quantitative Risk Assessment (Pasman et al., 2009).

Unlike safety-related accidents, however, security-related events are intentional and sometimes well-planned. Process security-related events may also cause harm to human health, loss of life, and major asset damage. Incidents such as the Saudi Aramco drone attacks (2019) and the Toulouse fertilizer plant explosion (2001)[1]emphasize the need for effective process security risk assessment and management to better protect CPI facilities against external threats, such as theft, sabotage, or acts of terrorism (Aven, 2007). Various techniques have been proposed and applied in the CPI context, including the Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF), and API Security Vulnerability Assessment Methodology (Matteini et al., 2019).

According to Khan et al. (2015), several review articles have been published that cover various aspects of process safety and risk management, including hazard identification, risk assessment and management, accident modelling, and inherent safety. They provided a historical development in this field and categorized the methods into qualitative, semi-quantitative, quantitative, and hybrid. Aven and Kristensen (2005) offered a unique perspective on risk analysis through the lens of different disciplines, such as engineering, economics, and social science; they also explored unified approaches to risk analysis. An examination of existing techniques for assessing risks was conducted by (Marhavilas et al., 2011) in research papers spanning from 2000 to 2009 across various work sites, with generic reference points being made throughout their article assessments. In subsequent years, Necci et al. (2015) conducted assessments on the quantitative risks associated with chemical processing plants, particularly concerning domino accidents, while Villa et al. explored in detail in 2016 the development of dynamic risk assessment.

Nonetheless, review articles focusing on process security risk assessment in the CPI are relatively scarce. In 2017, Baybutt highlighted the issues surrounding security risk assessment in the process industries, including theoretical foundation, the modelling of security risks, and the methods used. He emphasizes the need for rigorous and intelligent risk analysis that can inform decision-making and risk management. Moreover, in a comparative study conducted by Matteini et al. (2019), five Security Vulnerability Assessment (SVA) methodologies were identified, and two of them were discussed and compared in terms of their applicability in the CPI context.

Meanwhile, applying the resilience engineering paradigm is gradually being explored as an approach to provide a safety net in CPI (Jain et al., 2018a; Pasman et al., 2020a; Yarveisy et al., 2022). In the broad sense, resilience is a system's ability to maintain or achieve desired functionality following some event (Logan et al., 2022). In resilience engineering, a system is said to be resilient if it can adjust its functioning before, during, or following changes and disturbances and sustain required operations under expected and unexpected conditions (Hollnagel et al., 2012). Resilience engineering aims to enhance a system's capabilities to absorb, adapt, and recover from disruption and reduce the impacts of the disruptions on the system's performance (Chen et al., 2023; Hosseini et al., 2016). Therefore, the process resilience concept not only focuses on reducing the likelihood and consequence of failures but also on enhancing the system's ability to absorb and recover from shocks. It goes beyond traditional risk management by considering how quickly and effectively an organization can adapt to unexpected changes or recover from disasters (Hickford et al., 2018; Jain et al., 2018a). Currently, several resilience assessment methodologies have been proposed and developed for managing socio-technical systems in the face of

Table 1
Comparative overview of the type of risk between safety and security (Casson Moreno et al., 2018; Landucci et al., 2020; Meyer and Reniers, 2022).

	Safety	Security
Type I risk	**Occupational safety** E: Falling, slipping, minor fires C: Injury, a few fatalities, minor asset loss L: High	**Physical security** E: Petty theft, minor security breaches C: Injury, a few fatalities, minor asset loss L: High
Type II risk	**Process safety** E: Unintentional release of large hazardous materials, fires, and explosion C: Numerous fatalities, severe health effects, major asset loss & environmental damage L: Low	**Process security** E: Intentional release of large hazardous materials, fires, and explosion, terrorist attacks C: Numerous fatalities, severe health effects, major asset loss & environmental damage L: Low
Online risk	**Cyber safety** E: Accidental data deletion, unintentional software bugs C: Data loss, process & system downtime, potential minor financial loss L: High	**Cyber security** E: Hacking, phishing attacks, malware installation C: Data breach, financial loss, intellectual property loss, harm to reputation L: High

E = events, C = Consequences, L = likelihood

[1] It is not for sure, but it could have been security-related causes involved.

uncertainties, disturbances, and potential hazards in the CPI context, such as the Functional Resonance Analysis Method (FRAM), Process Resilience Analysis Framework (PRAF) and STAMP-based Quantitative Resilience Assessment (Jain et al., 2018b; Patriarca et al., 2017; Sun et al., 2022a,b).

1.2. Need for this review

In recognizing the complex landscape of risk management within the CPI, delineating the concepts of process safety, process security, and resilience becomes crucial. While intertwined, these domains address distinct aspects of risk management. Process safety primarily focuses on preventing and mitigating unintentional incidents and accidents, often with an emphasis on the probability of occurrence. For example, it involves assessing the likelihood of equipment failure or operator error. Process security, in contrast, concentrates on guarding against intentional threats such as sabotage or terrorist acts, focusing more on the attractiveness and vulnerability of systems or plants. Resilience extends beyond these, encompassing an organization's ability to adapt and recover from various disruptions, whether accidental or intentional. Differentiating these concepts is essential for developing targeted and effective risk management strategies. This study aims to explore these distinctions further, emphasizing the need for an integrated approach to managing process safety, process security, and resilience in the CPI.

It is evident from the literature that while studies on process safety risk assessment methods in the CPI have been extensive, there is a need for more research on process security risk assessment and resilience assessment methods in the CPI. To the best of the authors' knowledge, the interaction of process safety risk and process security risk in the CPI sector and their joint assessment using a resilience-based approach have not been extensively studied. However, it is crucial to consider the triplet process safety risk, process security risk, and process resilience when conducting a comprehensive risk assessment in the CPI sector. Therefore, this literature review not only synthesizes the existing methods of process safety risk assessment and process security risk assessment but also identifies opportunities for incorporating resilience concept and modelling approach to address the interaction between process safety and process security risks and treat them in an integrated framework.

Despite the importance of process safety risk assessment, process security risk assessment, and process resilience assessment in the CPI sector, there remains a gap in the literature on how these three areas may be synergized with each other. As such, this paper contributes to the literature by identifying existing methods for process safety risk assessment, process security risk assessment, and process resilience assessment in the CPI sector, highlighting their strengths and limitations, and identifying opportunities for future research that may integrate these three domains to address their interactions.

The importance of this study cannot be overstated, as it has the potential to significantly impact practitioners, researchers, and policymakers by providing them with valuable insights into the development and implementation of risk assessment and management strategies that can bolster the safety, security, and resilience performance of the CPI. By offering a comprehensive overview of the existing methodologies and highlighting their strengths and limitations, this review can contribute to the identification of knowledge gaps and opportunities for further research. Ultimately, this study aims to promote the continuous improvement of risk assessment practices and the prevention of major chemical plant accidents and deliberate attacks, ensuring the sustainability and resilience of the CPI in the long run.

1.3. Aim and scope of the review

The primary objective of this review is to discern the key methods used for assessing process safety risk, process security risk, and process resilience in the CPI. To comprehensively address this overarching research question, we will delve into five sub-research questions.

Initially, we delve into the literature to assess the current direction of peer-reviewed articles that encompass the themes of process safety risk assessment, process security risk assessment, and process resilience assessment in the CPI. Following this, we explore the literature to understand the fundamental concepts surrounding these three domains within the CPI. Subsequently, our focus shifted to identifying the specific approaches, techniques, and stages of assessment that have been employed in the domain of process safety, process security risk assessment, and process resilience assessment. Our fourth segment of exploration involves a critical evaluation of the strengths and limitations inherent to these methodologies. Concluding our investigation, we seek to identify promising trajectories for future research in these domains, particularly in the context of the CPI.

By answering these research questions, this systematic literature review offers a comprehensive and engaging analysis of the current state of process safety risk assessment, process security risk assessment, and process resilience assessment method within the CPI context. Through the identification and critical examination of the key methodologies, their applications, strengths, and limitations, we aspire to pave the way for a more holistic approach to managing process safety and process security risks, fostering sustainable growth and resilience in the CPI.

The structure of this paper is organized as follows: Section 2 outlines the methodology adopted for the systematic literature review (SLR), detailing the search strategy implemented. Section 3 presents the findings of our SLR, offering an overview of the fundamental concepts associated with process safety risk assessment, process security risk assessment, and resilience assessment within the CPI. This section further delves into the diverse approaches and stages of application of these assessment methods in the CPI context. Section 4 engages in a critical discussion, evaluating the strengths and limitations of these methodologies, especially when addressing process safety and process security risks, and resilience in the CPI. Subsequently, we will identify promising trajectories for future research in these domains. Lastly, in Section 5, we draw conclusions and put forth recommendations for subsequent research efforts.

2. Methodology

2.1. The review protocol

The present study adopts and uses the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) review protocol (Moher et al., 2009) as guidance. The PRISMA protocol aims to ensure that researchers provide appropriate and detailed information in their review. Nevertheless, the approach has been revised according to the dataset through dedicated protocols and data quality checks. Accordingly, we conducted a systematic literature review by formulating pertinent research questions for the review. Subsequently, we outlined the systematic search strategy, which encompassed three main sub-processes: identification, screening, and eligibility. We then appraised the selected articles based on their relevancy to our research questions. Finally, we described the process of abstracting the data for the review, as well as the methodology utilized to analyze and validate the abstracted data.

2.2. Formulation of the research question

This review included three main aspects, namely the chemical process industry (population); process safety and process security (interest); and risk assessment and resilience assessment methods (context), which then guided the authors to formulate the main research question, as stated before: *What are the key methods for assessing process safety risk, process security risk, and process resilience in the chemical process industries (CPI)?*

2.3. Systematic searching strategies

To identify relevant studies, the study's keywords were utilized in a search that was derived from the research question. These keywords included process safety and process security, risk assessment and resilience assessment, and the chemical process industry. To increase the relevance of results for the review, the search process employed synonyms, associated terms, and variations. Moreover, the identification procedure was informed by previous studies and keywords suggested by the selected database and industry experts. A complete search string was then developed, utilizing various search techniques, such as Boolean operators, phrase searching, truncation, wild cards, and field code functions, on the two primary databases, Web of Science (WoS) and Scopus. The search string for both databases is as follows: ((("process safety" OR "process security" OR "physical security") AND ("risk assessment" OR "risk analysis")) OR ("resilience assessment" OR "resilience analysis")) AND ("chemical industr*" OR "process industr*" OR "chemical plant*" OR "process plant*" OR "chemical facilit*" OR "process facilit*"). The search was conducted on March 14th, 2023, generating a total of 713 documents, which consist of 282 from WoS and 431 from Scopus, as demonstrated in Fig. 1.

2.4. Screening

To ensure comprehensive coverage, our initial search was extensive. In Scopus, using our defined search string, we found 45 records published between 1985 and 1999. Similarly, in WoS, the search yielded 11 records from 1992 to 1999. The strategic decision to commence our analysis from the year 2000 was aimed at capturing the most recent and relevant developments in these fields. This timeframe aligns with significant advancements and shifts in the CPI over the last two decades, particularly following major global events such as the 9/11 attacks. These events have markedly influenced technological innovations, regulatory changes, and security threat perceptions, making the post-2000

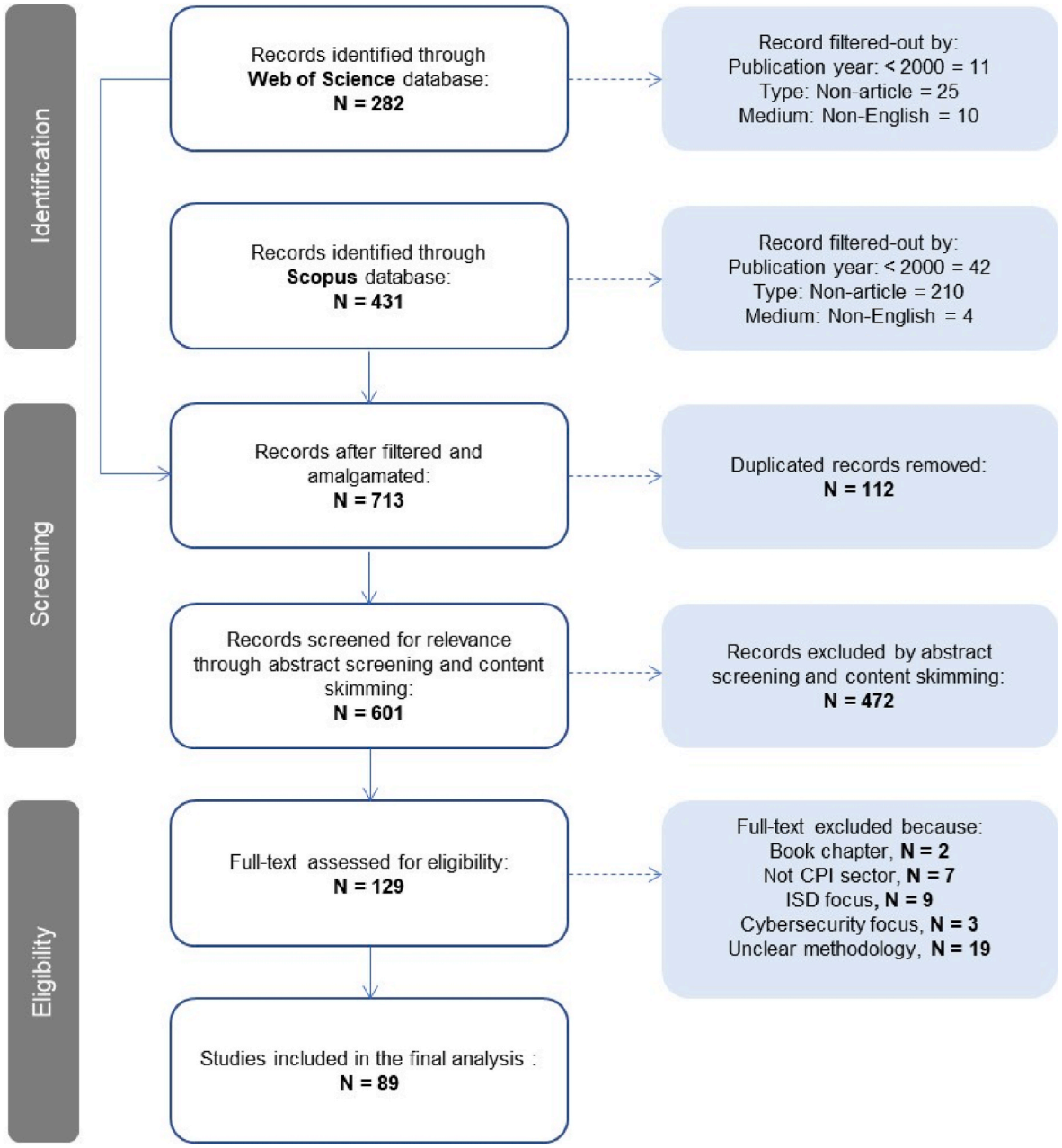


Fig. 1. Systematic literature review flowchart. Adapted from PRISMA 2020 Method.

literature particularly pertinent for understanding the current state and future directions in process safety, process security, and resilience.

During the screening phase, it was noted that the number of studies on process safety, process security, and resilience risk assessment methods has steadily increased since 2000. However, this study did not include articles published in 2023 (N = 8) during the search because a whole year was not completed. Consequently, articles published between 2000 and 2022 were selected as one of the inclusion criteria for this study. To minimize misunderstanding, the review incorporated only articles published in English. Other inclusion and exclusion criteria are listed in Table 2. Both records from WoS and Scopus were then amalgamated in the Zotero | Your, 2023 reference manager, and duplicate articles were removed in this process. We then carefully screened the records by title, abstract, and keywords corresponding to our criteria, resulting in 129 remaining articles being deemed eligible for the subsequent review stage.

2.5. Eligibility

The third stage of the review process is eligibility, during which we manually scrutinize the retrieved articles to ensure their compliance with the inclusion and exclusion criteria. This was carried out by carefully reviewing the article's content. The elimination of articles was based on several factors, including an unclearly defined methodology section, a primary focus on cybersecurity rather than process security, and the inclusion of studies conducted in non-chemical process industries and those published solely as book chapters. Consequently, 40 articles were excluded, and 89 were selected for further review.

2.6. Data extraction and analysis

We developed a spreadsheet for data extraction to provide consistency and thoroughness. The items covered in the form include the authors, the year the study was published, the type, techniques, and tools for risk and resilience assessment methods, the stage of assessment, and their primary data sources. The form also included sections for documenting the strengths and weaknesses of the methods used in the study, as well as any limitations disclosed by the authors.

Once the data extraction process was complete, the next step was to distil the collected information into thematic tables, creating a more coherent overview of the literature. At this stage, we divided the literature into four main categories: process safety, process security, integrated process safety and security, and process resilience assessment. We then coded the studies based on the techniques and tools used in the assessment methods and visualized them using Flourish web-based applications (Flourish Flourish, 2023).

Table 2
Inclusion and exclusion criteria for the screening and eligibility process.

Criteria	Inclusion	Exclusion
Timeline	2000–2022	<2000, >2022
Document type	Article and review	Book chapters, book series, conference proceedings
Language	English	Non-English
Type of industry	Chemical process industries	Non-chemical process industries
Focus of interest	Methodology on process safety risk assessment, process security risk assessment, and resilience assessment	Generic process safety management, Unclear methodology, Focus solely on cybersecurity, Focus solely on the early design stage of the chemical plant, Focus on natural disaster-related as main causal factors

Given the diversity of study designs, we refrained from conducting a quality assessment of the studies. Instead, we concentrated on the relevance of the studies to our objectives. This was done to present a holistic overview and contribute to the overall credibility of our synthesis.

3. Results

3.1. Current trend of publications related to process safety, security, and resilience assessment in the CPI

Our search yielded 713 results, and after careful screening, we included 89 peer-reviewed articles in our study. Table 3 summarizes the most prominent publication titles, authors, and countries in process safety, process security, and resilience assessment research.

The Journal of Loss Prevention in the Process Industries leads the pack with 23 records and is ranked in Q2 quartile with an Impact Factor of 3.5 for 2022 by the Journal Citation Reports (JCR, 2023). It is followed by Process Safety and Environmental Protection (PSEP) and Process Safety Progress (PSP), each contributing 12 records. Significantly, PSEP holds a prestigious Q1 quartile ranking and an Impact Factor of 7.8. Although PSP is in the Q4 quartile, it still maintains an Impact Factor of 1.0. Notably, Reliability Engineering and System Safety, and Safety Science also hold Q1 rankings, further emphasizing the high quality and critical importance of research in this area. Overall, the elevated Impact Factors and strong JCR quartile rankings of these journals highlight the rigor and significance of the ongoing research in this field.

The most prolific authors in this field are Khan F with 12 articles, Mannan MS with 8, and Yang M with 7. The United States is the leading contributor with 25 papers, followed by Canada with 13 and the People's Republic of China with 10. Other countries like India, the Netherlands, Italy, Kazakhstan, Belgium, Greece, and Norway also show active contributions, indicating a wide global interest in this research area.

As shown in Fig. 2, from 2000 to 2022, the publication landscape related to chemical process industries reveals evolving research priorities. Process safety has consistently maintained focus throughout, with publications gradually growing, particularly from 2017 onwards. This surge may be influenced by factors like increasing industrial complexities, and evolving safety standards and regulations. On the other hand, the process security's publication trend appears to be more sporadic, with initial activities in the early 2000s followed by a dormant period, hinting that the security aspect might have been relatively underresearched. However, only in 2019, a focus on integrating process safety and process security risk assessment in this sector started to emerge, indicating a newfound recognition of the importance of intertwining safety and security for comprehensive process plant protection.

Meanwhile, process resilience analysis has emerged as a steadily growing area since 2017. While this may suggest a growing industry interest in resilience against both anticipated and unforeseen challenges, including natural hazards triggering technological accidents (NaTech), we acknowledge that our study primarily focuses on academic literature and may not fully reflect industry trends. This observation points to the potential for more diverse and innovative research approaches to enhance industry robustness and resilience. Therefore, in the following sub-topics, we will look further at what have been described in these literature regarding process safety, process security as well as process resilience assessment methods in the CPI.

3.2. Overview of process safety risk assessment, process security risk assessment, and process resilience assessment methods

Risk assessment is a systematic process of understanding the nature of risk and evaluating the potential risks that may be involved in a projected activity with the available knowledge (Bjørnsen et al., 2020;

Table 3
Record count according to publication titles, authors, and countries (Top 10).

Publication Titles	JCR Quartile[a]	JCR, 2023	Record Count	Authors	Record Count	Countries	Record Count
J. of Loss Prevention in the Process Industries	Q2	3.5	23	Khan F	12	USA	25
Process Safety & Environmental Protection	Q1	7.8	12	Mannan MS	8	Canada	13
Process Safety Progress	Q4	1.0	12	Yang M	7	P.R. China	10
Reliability Engineering & System Safety	Q1	8.1	9	Jain P	6	India	9
Safety Science	Q1	6.1	7	Reniers G	6	Netherlands	9
Computers & Chemical Engineering	Q2	4.3	6	Cozzani V	4	Italy	8
Journal of Hazardous Materials	Q1	13.6	6	Gupta JP	4	Kazakhstan	5
IEEE Access	Q2	3.9	2	Bajpai S	3	Belgium	4
Sustainability	Q2	3.9	2	Moreno VC	3	Greece	4
Chemical Engineering Science	Q2	4.7	1	Pasman HJ	3	Norway	4

Notes:
JCR, Journal Citation Reports (JCR, 2023).
IF, Impact Factor.
[a] Highest quartile in a relevant JCR category.

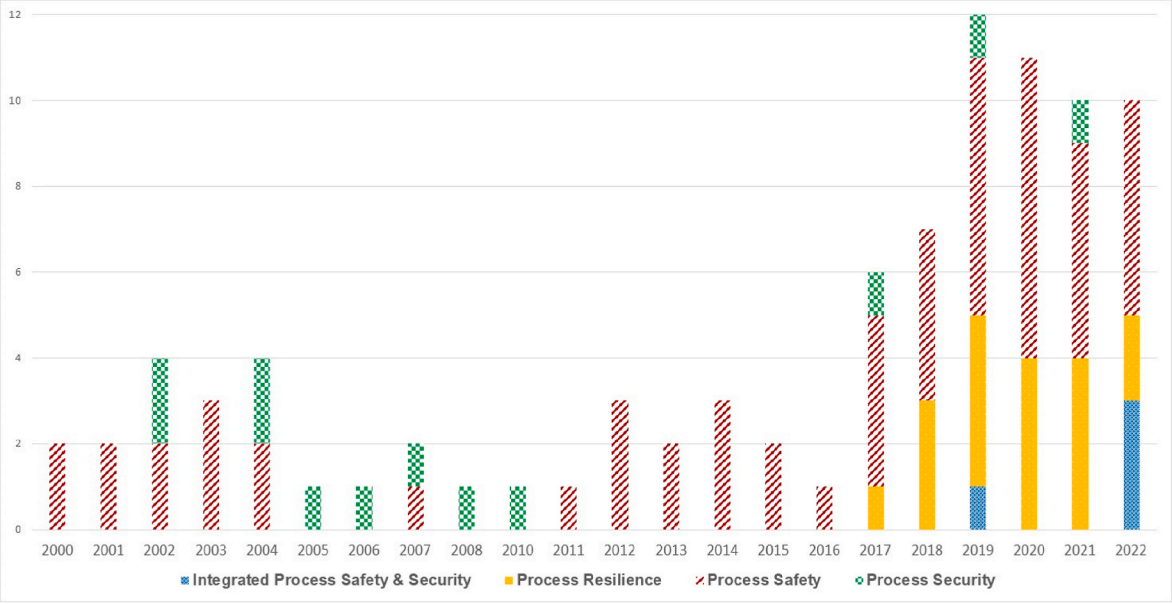


Fig. 2. Distribution of papers published between 2000 and 2022 across four domains.

SRA, 2018). It is the process used to understand the nature and determine the risk level by analyzing potential hazards and evaluating the possible impacts of occurrence. ISO 31000: 2018 provides a framework for risk management that is widely accepted and implemented across many sectors, including the CPI. Our review focuses on the first two stages of risk assessment (Fig. 3), part of this generic framework, which involves risk identification and risk analysis (estimation of consequences and likelihoods and risk calculation).

Risk is a concept that has several definitions and implications, depending on the perspective and the domain of application. A state-of-the-art review of risk definitions and assessment in CPI is presented by Villa et al. (2016). In short, risk is a measure of the uncertainty and severity of adverse effects of an event or an activity with respect to something that humans value, such as life, assets, and the environment (Villa et al., 2016). Risk can be expressed in different ways, such as expected loss, probability of an event, and potential of a loss. In terms of loss, the risk is assessed by combining the probability that the loss would happen and the potential loss due to an abnormal condition (Wang et al., 2016). Risk can be assessed and managed using different methods and criteria, depending on the context and the objectives. In the process safety domain, risk is often measured by the likelihood (probability in quantitative terms) of an event and its severity of consequences. Put simply, **Process safety risk = Probability x Consequence** (Adedigba et al., 2018; B et al., 2020; Guo et al., 2018).

Meanwhile, in the process security domain, several scholars and organizations presented the definitions of risk, commonly defined by threat, vulnerability, and consequence, without any explicit reference to a probabilistic component (Cox, 2008; Reniers et al., 2008). However, Amundrud et al. (2017) analyzed the compatibility between safety and security risk frameworks, concluding that also security risk may be defined by events-consequences and uncertainties as in the case of safety risk. Moreover, Kriaa et al. (2015) suggest that probabilities are a suitable way to express these uncertainties, particularly in a given scenario of attack, which provides a clearer context for understanding process security risks.

As highlighted by Landucci et al. (2020) and Matteini et al. (2019), systematic methodologies for process safety risk assessment have been developed over the past forty years to address the growing complexity within the CPI, culminating in established practices like dynamic Quantitative Risk Assessment (QRA). In contrast, the evolving nature of type II process security risks has not been as thoroughly addressed, as process security risks can shift dramatically based on unpredictable socio-political events. The effort of evaluating risks associated with potential terrorist attacks on industrial sites is especially complex for several reasons. Firstly, there is a limited historical precedent of terrorist activities targeting chemical process installations. Secondly, a multitude

Fig. 3. Overview of risk management process (ISO 31000, 2018).

of external elements can either amplify or mitigate these security risks. Lastly, the factors that influence these security (and safety) risks are not static; they interact in a dynamic manner and evolve over time, as noted by Landucci et al., (2020) and Moreno et al. (2018).

Therefore, the early literature on process security risk assessment largely presents speculative and qualitative insights. Historically, the emphasis on this subject grew after the 9/11 attacks, leading to the creation of Security Vulnerability Assessment (SVA) methods by the American Petroleum Institute (API) and Center for Chemical Process Safety (CCPS), both first published in 2003. CCPS (2003) defines security risk as the likelihood of an adversary or threat successfully exploiting a specific vulnerability of a particularly attractive target, resulting in a degree of damage or impact on an asset. Similarly, the ANSI/API Standard 780 defines security risk as a "function of the Consequences of a successful attack against an asset and the Likelihood of a successful attack against an asset" (Moore, 2013). As explained by (Landucci et al., 2020), the "likelihood of a successful attack" can be equated to vulnerability (V). Additionally, the anticipated consequences can be viewed as a blend of the "attractiveness of the asset to the threat" (A) and the "threat" (T) parameter. This is because the greater the anticipated consequences, the more enticing an asset becomes to a potential adversary, increasing its threat level. Moreover, Consequence (C) denotes the "worst-case consequences" or the impact value associated with the security risk. Put simply, **Process security risk = V x (A x T) x C.**

Progressively, there are a handful of semi-quantitative methodologies that have been introduced or utilized in real-world scenarios for process security risk assessment across various facilities. Common factors considered in these methodologies encompass threat levels, the attractiveness of the facilities to adversaries, potential consequences and repercussions of an incident, and the vulnerability level (Bajpai and Gupta, 2005). While there are subtle variations across different methodologies, a general step-by-step procedure is discernible, which encompasses the primary stages outlined in Table 4.

However, Reniers et al. (2020) argue that process safety and process security are intertwined, the only difference being the human intention of causing the losses. They explain that a protection or prevention barrier in case of process safety, and a countermeasure in case of process security, is required to prevent a hazard or a threat that may become out

Table 4
SVA methodologies for the chemical and petrochemical industry (adapted from (Landucci et al., 2020; Matteini et al., 2019).

Step	Description	Method and reference			
		Jaeger (2002)	CCPS (2003)	Bajpai and Gupta (2005)	(API - Moore, 2013)
1	Facility characterization	✓	✓	✓	✓
2	Threat identification	✓	✓	✓	✓
3	Attractiveness analysis				✓
4	Vulnerability analysis	✓	✓	✓	✓
5	Risk assessment	✓	✓	✓	✓
6	Risk mitigation and countermeasure	✓	✓	✓	✓

of control from reaching the target (Fig. 4). Furthermore, there are strong motivations for unifying process safety and process security risk management in the CPI, as highlighted by Ylönen et al. (2022). They mention at least four reasons, which include the recognition of mutual interactions and influences between safety and security risks, the avoidance of conflicts arising from competing goals and logics, the economic benefits of cost-efficiency and synergies, and the need to identify and mitigate systemic risks of the convergence of process safety and security risk. Nevertheless, as pointed out by (Ylönen et al., 2022), the current state of the integrated management of safety and security (IMSS) in Seveso plants is still in its infancy, as process security is often handled separately from process safety, and the communication and coordination between different experts and organizational units are inadequate.

On the other domain, (process) resilience refers to the ability of a process system to restore performance after sustaining severe damage by a usually unforeseen threat or hazard, making it capable of absorbing disturbances or changes (Pasman et al., 2020b). It is central to the concept of resilience engineering, combining technical and social factors to withstand (high) consequence events (H. Pasman et al., 2020b; Zinetullina et al., 2021). These assessments typically evaluate a system's ability to absorb, adapt to, and recover from unexpected disruptions through the implementation of appropriate measures (C. Chen et al., 2021; Vairo et al., 2020).

However, Jain et al. (2018a) point out that process systems resilience needs to be more standardized and quantifiable. Drawing inspiration from Hollnagel's foundational principles of resilience engineering (anticipation, monitoring, response, and learning), (Jain et al., 2017) outlined four elements for a process resilience analysis framework. These elements encompass early detection (spotting weak signals via vigilant monitoring and anticipation), error-tolerant design designs that are forgiving to errors (incorporating inherently safer design principles), plasticity (often described as resistive adaptability), and recoverability, as shown in Fig. 5.

To this point, there are similarities and differences between process safety risk assessment, process security risk assessment, and resilience assessment, as summarized in Table 5. Process safety risk Assessment primarily focuses on managing risks associated with accidents resulting from unintentional events, such as equipment failure, human error or human violations. For instance, Process Hazard Analysis (PHA), often conducted using methods like HAZOP, is an essential step in identifying potential hazards and mitigating the associated risks (Chastain et al., 2017; J. Y. Choi and Byeon, 2020; Venkatasubramanian et al., 2000). This approach has a well-established process for defining risk tolerance criteria, identifying hazardous scenarios (mainly static), and applying a probabilistic perspective to calculate risks. An example might be identifying a potential equipment failure that could lead to a chemical leak and then designing safety measures such as redundancy or automatic

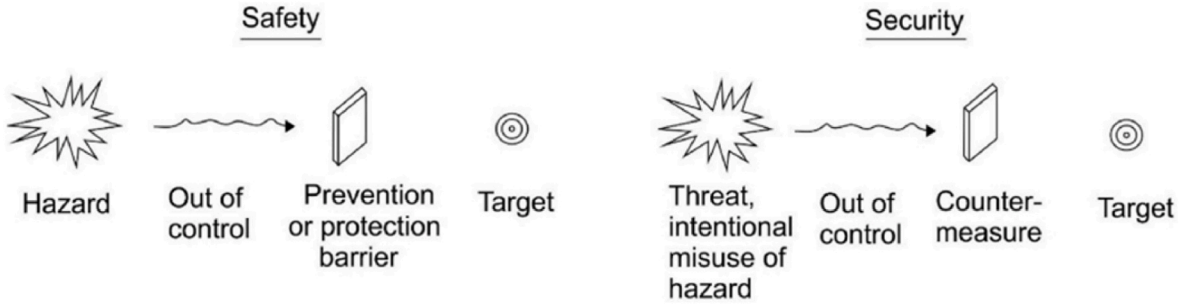


Fig. 4. Constitutive elements of process safety risk and process security risk (Reniers et al., 2020).

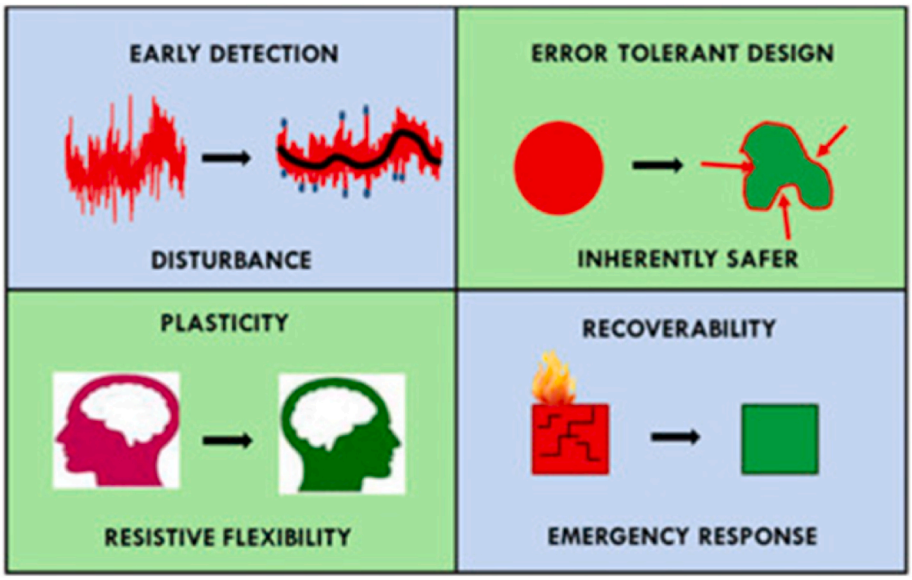


Fig. 5. Elements of process resilience (Jain et al., 2017).

shut-off systems to prevent this scenario (Marhavilas et al., 2020; Penelas and Pires, 2021; Ramzan et al., 2007).

On the other hand, process security risk assessment aims to address malevolent incidents with the purpose of causing losses, such as deliberate attacks on a facility, which are inherently more dynamic and unpredictable. An essential tool in this process is the Security Vulnerability Assessment (SVA), which identifies potential threats, determines their likelihood, and develops strategies to mitigate their impact (Dunbobbin et al., 2004; Lemley et al., 2003). Unlike safety risk assessment, security risk assessment often deals with less well-defined risk tolerance criteria and the difficulty of conclusively identifying all potential threats (Bajpai and Gupta, 2005). Here, a possibility theory perspective is often adopted, where scenarios are evaluated based on the possibility of occurrence rather than probability. A classic example would be the anticipation of (cyber)attacks on the control systems of a chemical plant and the implementing appropriate (cyber)security measures (Amin et al., 2022; Iaiani et al., 2021; Song et al., 2019).

Resilience assessment, the third pillar in our comparison, offers a unique perspective. Rather than focusing solely on preventing specific hazard or threat scenarios, it addresses the system's overall ability to absorb disturbances and reorganize (Sun, et al., 2022; Vairo et al., 2020), whether they result from unintentional accidents or deliberate attacks. This means it must consider both defined and undefined risk scenarios, focusing on system adaptability. Time is a crucial factor, emphasizing system recovery and reorganization over time (Jain et al., 2019a,b; Sun et al., 2022a,b). A resilience perspective might consider how a system can flexibly adapt to unexpected disruptions, for example, by rapidly adjusting production processes or re-routing materials in response to disruption from process unit failures, human errors, cyber-physical attacks, and natural hazards, among others (Jain et al., 2019a,b; Sun et al., 2022a,b; Zinetullina et al., 2020).

Despite their distinct focus areas, these three assessment methods share a common goal: to safeguard the operations of CPI from various risks, whether unintentional or deliberate, and ensure the system's resilience amidst unforeseen challenges. By complementing each other, they together provide a comprehensive, multi-faceted approach to risk management in the CPI. Therefore, understanding their unique contributions and limitations can lead to a more robust and resilient chemical process industry.

3.3. *Type of approach, tools, and stage of assessment*

Our comprehensive analysis, as in **Appendix A**, has categorized the assessment methods into three distinct categories: qualitative, quantitative, and semi-quantitative. The distribution of these approaches across different assessment areas is visually represented in Fig. 6.

The qualitative approach, accounting for 12% overall, is anchored in subjective evaluations. It capitalizes on expert judgments to discern and prioritize risks. Given its reliance on human expertise and experience, this method is particularly apt for areas where data might be limited or where the nature of the risk is inherently unpredictable. A case in point is the process security domain, where a significant 58% of its methods are qualitative-based. This pronounced inclination towards expert judgment could stem from the unpredictable nature of security threats,

Table 5
Comparison between process safety risk assessment, process security risk assessment, and resilience assessment (Baybutt, 2017; Reniers et al., 2020; Varadharajan and Bajpai, 2023; Yang et al., 2023).

Process Safety Risk Assessment	Process Security Risk Assessment	Resilience Assessment
Addresses accidents resulting from unintentional acts	Addresses malevolent/ incidents with an **intentional attack**	Addresses the capacity of a system to **absorb disturbance** and reorganize
Relates to Process Hazard Analysis	Relates to **Security Vulnerability Assessment**	Relates to **system flexibility** and adaptability
Risk tolerance criteria are properly addressed	**Risk tolerance criteria are not properly defined** but are discussed	**Considers both defined and undefined risk scenarios**, focusing on the system's ability to adapt
More information is available to identify hazardous scenarios	**Relatively difficult to make absoluteness in the identification of threats**	Evaluates capacity for **identification and management of both known and unknown threats**
Hazard scenarios are mostly static **but inherently involve dynamic elements such as the flow of liquid and dispersion of vapor.**	**Threat scenarios are dynamic**	**Assesses both static and dynamic scenarios**, focusing on the ability to adapt to changes
The hazardous situation remains constant**, and time plays no significant impact**	**The threat may vary over time**	**Time is a crucial factor** as it focuses on system recovery and reorganization over time
Black swan events are rare	**Black swan events are highly possible**	Focuses on **preparing for and recovering from black swan events**
Calculated based on probabilistic theory perspective	Calculated mainly on the **possibility theory perspective**	**It uses a systems perspective** and may incorporate elements of both probabilistic and possibility theories

especially when one factor in elements like human intent is inherently challenging to quantify.

Conversely, the quantitative approach, which makes up 34% overall, is rooted in mathematical models and statistical analyses. It seeks to quantify risks based on empirical data, making it especially relevant in areas flush with data and where risks can be numerically articulated. A notable observation is the integrated process safety and security domain, where 75% of its methods are quantitative. This suggests a pronounced tilt towards data-driven assessments when jointly considering safety and security. However, it is crucial to note that the sample size for this domain is relatively small (N = 4), which might limit the robustness of this observation.

The semi-quantitative approach, representing 54% overall, bridges the gap between the qualitative and quantitative paradigms. It melds elements from both, employing numerical scales or categories to evaluate risks. This balanced perspective is particularly beneficial in domains with a mix of available data and a need for expert judgment. The process safety domain, with 64% of its methods leaning semi-quantitative, seems to thrive on this balanced approach, likely due to its numerous risks, ranging from equipment malfunctions to human errors. Similarly, the process resilience domain is strongly inclined towards the semi-quantitative approach, highlighting the intricate balance between data-driven insights and expert judgment in ensuring adaptability and robustness against unforeseen challenges.

While each domain exhibits its unique assessment approach, the overarching trend leans towards semi-quantitative approaches. This suggests a broader industry preference for methods that combine the rigor of quantitative data analysis with the flexibility and context provided by qualitative expert judgment. The emphasis on semi-quantitative methods in process safety and resilience domains underscores the complexity and multifaceted nature of risks in these areas, necessitating a more balanced approach. On the other hand, the heavy reliance on qualitative methods in the process security domain indicates the challenges in predicting and quantifying security threats, making expert judgment invaluable.

Building on our previous analysis, the techniques or tools employed in these assessment methods are intrinsically tied to the approach adopted. Qualitative approaches predominantly lean on tools like checklists, expert interviews, and brainstorming sessions, all aimed at discerning and prioritizing risks. Quantitative approaches, in contrast, harness tools such as fault tree analysis (FTA), event tree analysis (ETA), and Monte Carlo simulations, offering a mathematical lens to risk assessment. Bridging the two, semi-quantitative approaches deploys hybrid tools like Layer of Protection Analysis (LOPA) and Bayesian Networks, which seamlessly blend qualitative insights with quantitative rigor.

To provide a clearer perspective, we have crafted a visual representation depicted in Fig. 7, showcasing the diverse techniques or tools favored by researchers across the domains under scrutiny. It is worth noting that the circle size in this representation is proportionate to the number of studies within each domain. Within the process safety domain, predominant techniques encompass Hazard and Operability Study (HAZOP), Bayesian Networks (BN), Fault Tree Analysis (FTA), Bowtie, and Layer of Protection Analysis (LOPA). In the domain of process security, techniques such as Security Vulnerability Assessment (SVA) and risk matrix find frequent applications. When researchers develop integrated process safety and security risk assessment methods, the techniques are mainly combinations of BN, FTA, and Event Tree Analysis (ETA). Meanwhile, in process resilience assessment, the spotlight is on methods rooted in the BN, Functional Resonance Analysis Method (FRAM), Process Resilience Analysis Framework (PRAF), Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA), and System-Theoretic Accident Model and Processes (STAMP).

Diving deeper, the assessment stage of these assessment methods can vary depending on the specific needs and objectives of the studies. We have dissected how those studies deploy the assessment methods at different stages, including hazard identification, likelihood or vulnerability analysis, consequence analysis, and overall risk calculation or estimation.

Certain techniques (or studies) focus on only one stage of the assessment process, while others incorporate multiple stages. For example, techniques such as the (early) HAZOP are commonly used during the hazard identification stage to identify potential hazards and their consequences. In comparison, Event Tree Analysis (ETA) and Monte Carlo simulation are commonly used for probability analysis in the quantitative approach. Some techniques are broad enough to cover multiple stages of the assessment process, such as LOPA, BN, STAMP, and FRAM, which combine with other tools to cover hazard identification, likelihood analysis, consequence analysis, and overall risk. The selection of risk assessment techniques, however, depends on several factors, including the type of risk being considered, the availability and reliability of data, the nature and complexity of the process, and the specific objectives of the assessment.

4. Discussion

4.1. Strengths and limitations of process safety, security, and resilience assessment methods

Our analysis, building on the results from the previous sections, highlights that methods such as BN, Bow-tie, ETA, FRAM, FTA, HAZOP, LOPA, PRAF, RIPSHA, Risk Matrix, STAMP, and SVA are frequently employed to address concerns related to process safety, process security and/or process resilience in the CPI. In this section, we further analyze the strengths and limitations of these 12 methodologies and their

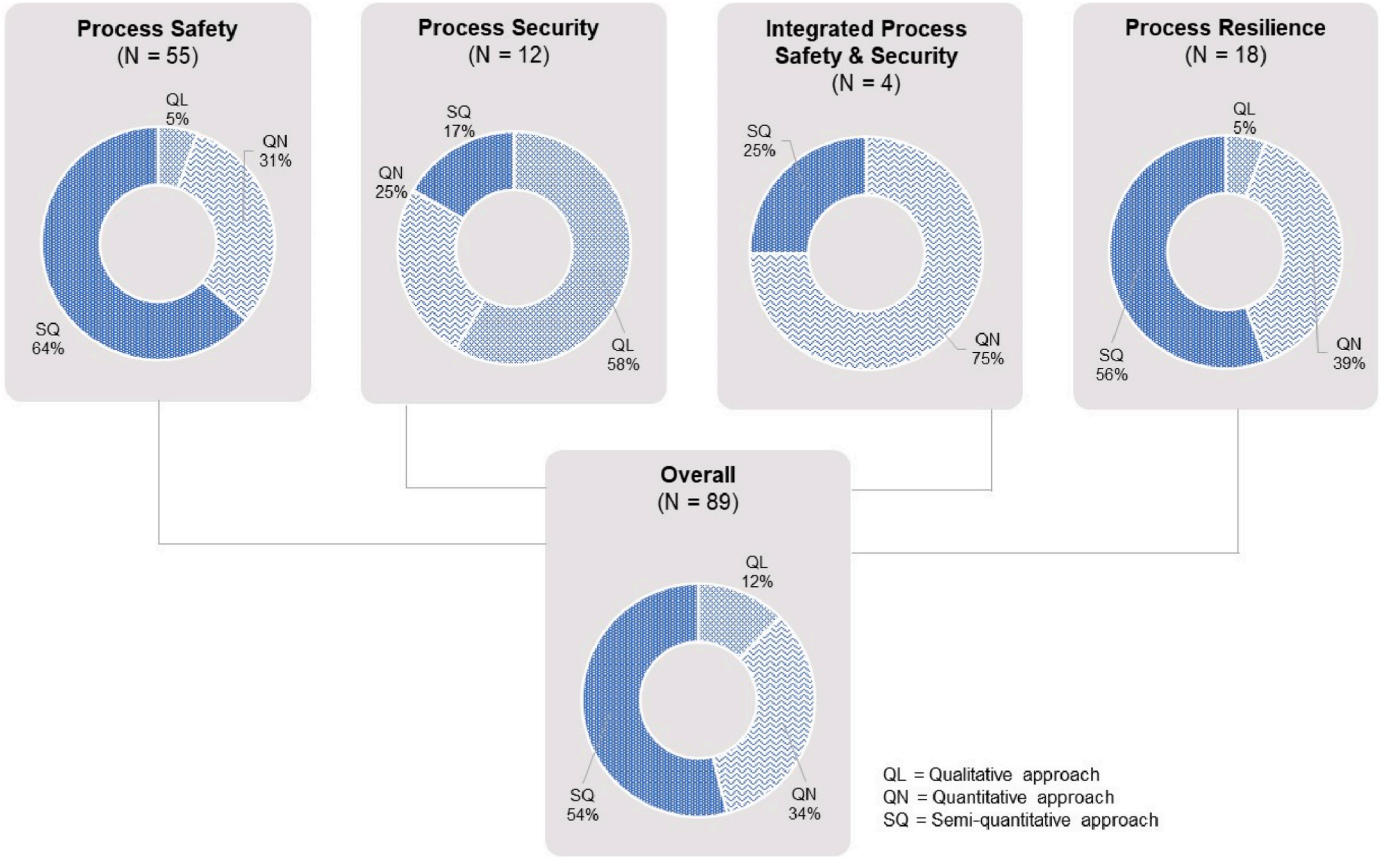


Fig. 6. Distribution of assessment approach across different domains.

applicability within the process safety, process security, and process resilience domains. The insights are summarized in Table 6.

The diverse methodologies and tools available for risk assessment in the CPI underscore the industry's multifaceted nature and the challenges it faces. The choice of method often reflects the specific challenges and objectives of a given study or application. For instance, while HAZOP is a mainstay for hazard identification in process safety, its limitations in addressing intentional security threats highlight the need for more specialized tools in the process security domain. The prominence of semi-quantitative methods, as evidenced in our earlier analysis, suggests a broader industry preference for a balanced approach. This balance, which combines the rigor of quantitative data analysis with the flexibility and context provided by qualitative expert judgment, is particularly relevant in an industry where risks can be both well-defined and highly unpredictable.

However, in discussing semi-quantitative risk assessment methodologies, it is important to recognize that these approaches range from simple to detailed analyses. Effective semi-quantitative assessments should encompass comprehensive coverage of relevant hazards and scenarios, utilize validated data and assumptions, and apply a consistent scoring system that will require expert judgment. The involvement of diverse stakeholders and clear documentation of the assessment process enhance the robustness of these methodologies. Regular review and updates are crucial to maintain their relevance in dynamic operational environments.

Moreover, the integration of safety and security, although still in its infancy, is gaining traction. This is evidenced by the emergence of methodologies that cater to both domains, such as the BN-based and FTA-based methods. Such integrated approaches recognize the intertwined nature of safety and security risks and aim to provide a comprehensive assessment framework. Yet, challenges persist. Many of the methodologies, while robust in their design, rely heavily on expert judgment, data availability, and computational resources. This can pose challenges, especially for smaller entities within the CPI that may lack the necessary resources or expertise. Additionally, the dynamic and evolving nature of threats, especially in the security domain, means that risk assessment methodologies must be adaptable and regularly updated.

From our analysis, five methodologies, BN, FRAM, PRAF, RIPSHA, and STAMP, stand out as particularly promising for a holistic approach to process safety, security, and resilience within the CPI.

BN-based methods excel in managing uncertainty and complexity, which is essential for addressing safety, security, and resilience. BN's graphical models offer clear visualization of causal relationships, and its probabilistic nature facilitates informed decision-making amidst uncertainty. While BN's dynamic risk management capability is advantageous for the ever-evolving CPI landscape, its data-intensive nature and the need for specialized expertise can be limiting, especially when relevant data is scarce.

FRAM, rooted in sociotechnical systems, emphasizes variability and the ability to model intricate interactions, making it apt for the CPI's interconnected processes. Recognizing variability as a standard performance aspect, FRAM aligns with resilience, underscoring adaptability. However, its qualitative nature demands a profound understanding of system functionality, which can be challenging for expansive systems.

PRAF adopts a systems perspective, highlighting the interplay of technical and social factors in process systems. It accentuates early hazard detection and the system's adaptability post disruptions. While PRAF offers a comprehensive resilience view, challenges like quantifying social factors and data needs persist.

RIPSHA, grounded in sociotechnical systems, offers a holistic approach to process safety and potential process security. It captures the nuances of modern socio-technical systems, emphasizing interactions and interdependencies. While RIPSHA integrates resilience engineering

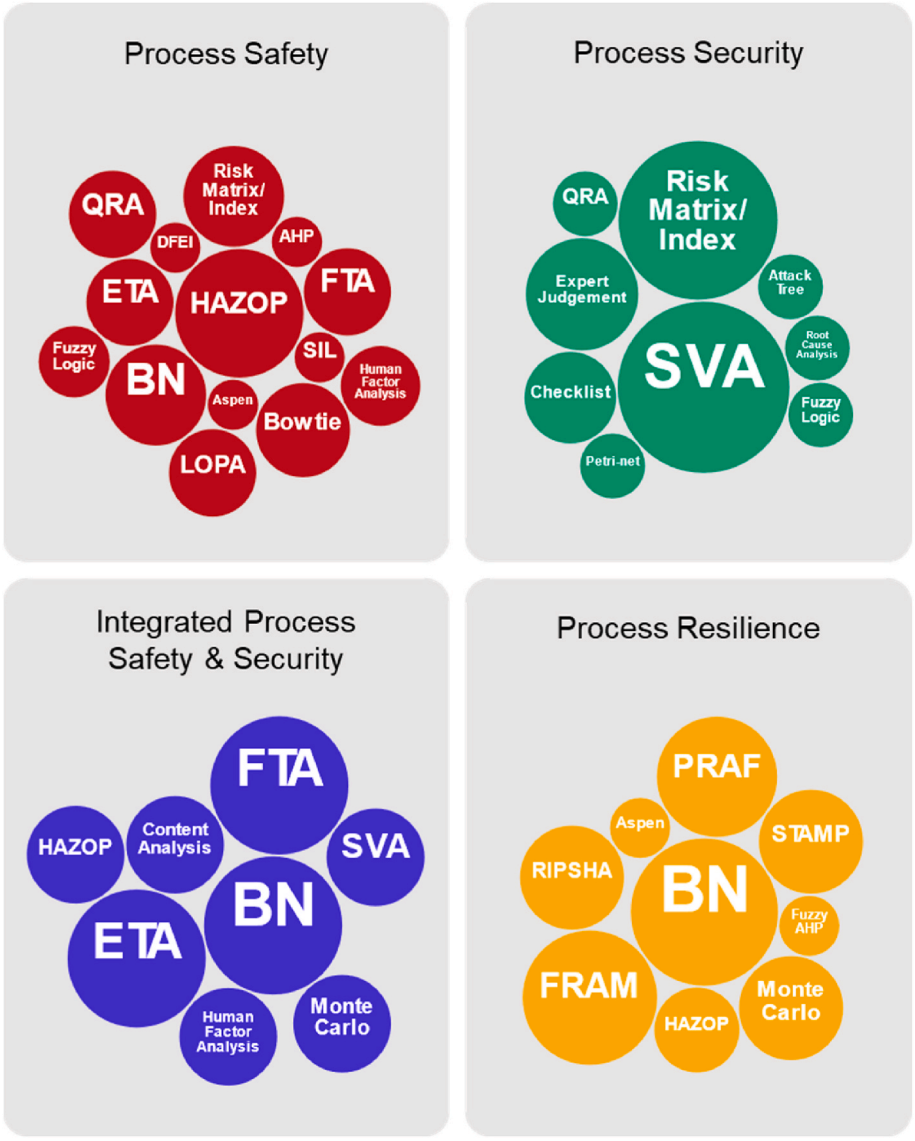


Fig. 7. Main process safety and process security risk, and process resilience assessment techniques employed in the CPI (the size of the circle is relative to the number of studies in the same domain).

concepts, its reliance on expert judgment and the need for extensive data are areas of concern.

STAMP also offers a systems-based perspective, weaving in technical, human, and organizational elements. Its proactive strategies, emphasizing control and feedback mechanisms, align with the CPI's dynamic nature. However, its abstract nature and limited real-world applications might challenge its broader adoption.

Pasman and Rogers (2015) advocate the significance of a systems approach to gain a holistic view of intricately engineered systems. They further stress the urgency for more research and practical tools to implement this perspective. Concurrently, while each method offers unique strengths, they all emphasize a system-oriented approach, crucial for managing the intricacies of process safety, process security, and resilience. Leveraging these methods in tandem could offer a comprehensive view of risks, paving the way for robust risk management in the CPI. Despite their limitations, these methodologies provide invaluable insights for the CPI. An integrated approach, capitalizing on their strengths and addressing their weaknesses, could be the key to effective risk management in this dynamic sector.

4.2. *Future research*

Our comprehensive investigation has highlighted a distinct shift in research trends, gravitating towards more dynamic and systemic-based assessment methods. Notably, methodologies like FRAM, RIPSHA, and STAMP are gaining traction, reflecting the industry's growing recognition of the need for holistic and adaptable risk assessment frameworks that can address the multifaceted challenges of sociotechnical systems within the CPI.

However, despite these advancements, two significant literature gaps have been identified: (1) the integration of resilience paradigms within process security domains and (2) the integration of resilience paradigms within frameworks that address both process safety and process security. In the context of process safety, process security, and resilience, resilience refers to the system's ability to anticipate, absorb, adapt to, and rapidly recover from potential disruptions. This paradigm emphasizes not just the prevention of adverse events but also the capacity to bounce back and even thrive after disturbances. It is a forward-looking approach that values adaptability, learning, and continuous improvement.

The absence of a resilience-centric focus in the current literature

Table 6
Analysis of strengths and limitations of main assessment methods for addressing process safety (Safe.), process security (Sec.), and resilience (Res.).

Method	Strengths	Limitations	Applicability			Main References
			Safe.	Sec.	Res.	
Bayesian Network-based	• Incorporates prior knowledge even with sparse data. • Dynamic risk assessment suitable for analyzing complex CPI systems. • It can be updated in real time or as new info becomes available.	• Sensitive to choices of prior probabilities. • Heavy computational requirements, especially for large systems. • May face challenges in validation and verification.	x	x	x	(Amin et al., 2022; Baksh et al., 2015; Kanes et al., 2017; Roy et al., 2014; Song et al., 2019)
Bowtie-based	• Visual representation of relationships between hazards and threats. • A comprehensive approach to both intentional and unintentional threats. • May integrates resilience engineering concepts.	• Might overlook certain scenarios. • Relies on expert judgment and estimations. • May miss interdependencies between different bow-ties.	x			(B et al., 2020; Guo et al., 2018; Santana et al., 2022; Schmitz et al., 2021)
ETA-based	• Systematic visualization of event sequences. • Quantifies the probability of different outcomes. • Useful for understanding the progression of events.	• Requires a clear initiating event. • It may not capture all possible event sequences. • Relies on accurate probability data for each event.	x	x		(Chen et al., 2020; Fang et al., 2020; Kim et al., 2003; Moreno et al., 2022)
FRAM-based	• Focuses on variability and performance in systems. • Highlights the impact of variability on safety and security. • Aligns with resilience through adaptability focus.	• Requires a deep understanding of system functionality. • Its qualitative nature can be complex to incorporate in traditional methods. • Limited practical implementation examples.	x	x	x	(Bjørnsen et al., 2020; Menezes et al., 2021; H. J. Pasman et al., 2018; Yousefi et al., 2019; Zinetullina et al., 2021)
FTA-based	• Graphical representation of the combinations of failures leading to an undesired event. • Quantitative method that can calculate the probability of the top event. • Helps in identifying the root causes of failures.	• Can be complex for large systems. • Requires accurate and comprehensive failure data. • It might not capture dynamic interactions in the system.	x	x		(Aneziris et al., 2014, 2017; Krishna et al., 2003; Sano et al., 2020)
HAZOP-based	• Comprehensive identification and analysis of potential hazards. •Fosters interdisciplinary cooperation for a thorough assessment. •Highly systematic, ensuring comprehensive coverage of failure modes.	• Less precise for processes with intricate relationships. • Struggles with identifying intentional security threats. •Focuses on individual events over combinations.	x			(Ávila et al., 2013; Bartolozzi et al., 2000; Penelas and Pires, 2021; Ramzan et al., 2007)
LOPA-based	•Excellent for simplifying, quantifying, and prioritizing risk, providing a clear view of safety measures required. •Facilitates risk communication between different stakeholders.	•Less suitable for handling the unpredictable and qualitative nature of security threats, •Relies heavily on quantitative risk data.	x			(Chastain et al., 2017; Wagner and Champion, 2012; Wasileski and Henselwood, 2011)
PRAF	•A holistic method combining technical and social factors. •Enhances resilience and encourages a proactive safety culture. •Provides quantitative assessment using plant performance data.	•Lacks comprehensive comparison with other methods. •It might be computationally expensive for large systems. •Assumption constraints like the normal distribution of uncertain parameters.	x		x	(Jain et al., 2019; Jain et al., 2018a; Jain et al., 2019a,b; H. Pasman et al., 2020b)
RIPSHA	•Integrative method capturing technical, human, and organizational factors. •Grounded in resilience engineering. •Adaptable across chemical process plant life cycles.	•It might be resource-intensive and demanding. •There is no quantitative comparison with other hazard analysis methods. •Requires extensive data collection from varied sources.	x		x	(Jain et al., 2018a; Jain et al., 2018c; Pasman et al., 2020b)
Risk Matrix/ Index-based	•Rapid qualitative tool for prioritizing process safety risks. •Facilitates clear communication of risk. •It can be used for the initial screening of security risks.	•Potential oversimplification of security threats. •Might not grasp the dynamic nature of threats. •Relies on qualitative and subjective assessments.	x	x		(Bajpai and Gupta, 2007; Baybutt, 2017; Dunbobbin et al., 2004; Moore, 2006)
STAMP-based	•Views accidents as system failures, not just components. •Comprehensive in addressing human, organizational, and technical factors. •Strong for understanding resilience with a system-wide perspective.	•Lacks a formal mathematical foundation. •It may be subjective and qualitative in nature. •May miss specific vulnerabilities in large-scale systems.	x	x	x	(Cameron et al., 2017; Pasman et al., 2018; Sun et al., 2022a,b)
SVA	• Comprehensive evaluation of potential security threats. • Identifies vulnerabilities and suggests countermeasures. • Integrates both technical and human factors	• It might be subjective based on the expertise of the assessor. • Requires regular updates as threat landscapes evolve. • It may not capture all potential vulnerabilities.		x		(Bajpai and Gupta, 2005; Lemley et al., 2003; Moore, 2006)

suggests that while we are making strides in understanding and assessing risks, there is a missed opportunity in preparing systems to be more resilient in the face of unforeseen challenges. This gap is especially pertinent given the increasing complexity and interconnectivity of modern systems, where disturbances in one area can have cascading effects across the entire system.

Thus, future research should prioritize the exploration and integration of resilience principles into process safety and process security assessment methodologies. This research direction necessitates the establishment of clear, quantifiable metrics for measuring resilience that can be seamlessly integrated into comprehensive process safety and security risk assessment tools. Importantly, these tools should incorporate decision-making elements to guide operators and regulators in prioritizing interventions. It also calls for in-depth case studies to glean insights into the successful (or unsuccessful) real-world applications of resilience principles. Furthermore, there is a pressing need to create or refine tools that not only assess risks but also offer actionable insights on bolstering system resilience. Lastly, it is imperative to ensure that industry professionals receive adequate training and education, equipping them with the requisite knowledge and skills to weave triplets of process safety, process security, and resilience strategies into their operations. By addressing this literature gap, the CPI can move towards not just safer and more secure operations but also systems that are robust, adaptable, and resilient in the face of an ever-evolving landscape of risks and challenges.

5. Conclusion and recommendations

In the CPI, ensuring optimal process safety, process security, and resilience is paramount. Our research has highlighted a significant void in the current literature. There's a notable absence of studies integrating the resilience paradigm into a cohesive framework for process safety and process security risk assessment. Addressing this gap is not just beneficial but vital. A unified risk assessment framework not only offers a comprehensive approach to risk management but also aligns with the dynamic nature of the CPI, thereby ensuring a high level of protection for people, property, and the environment. While our findings highlight the growing importance of resilience measures in the chemical process industry, it is imperative to reiterate that these measures should complement, not replace, the thoroughness of risk assessments. Rigorous risk assessment remains the cornerstone of effective resilience management, ensuring a comprehensive understanding of potential hazards and informed decision-making.

Drawing from our comprehensive review, we advocate for the chemical industries to embed systems-based semi-quantitative risk assessment techniques within their safety, security, and resilience blueprints. Such techniques strike a balance between quantitative data and qualitative expert judgment, aptly suited for the complex and fluid risk environments inherent to the CPI. Unlike purely qualitative or quantitative methods, semi-quantitative techniques can adeptly capture both the uncertainty and variability of risk factors and the dynamicity of process systems, offering a more realistic risk assessment.

Furthermore, holistic management of process safety and process security risks necessitates the crafting and adoption of unified risk assessment frameworks. Such frameworks would ensure a comprehensive and integrated risk management strategy, encompassing both safety and security dimensions. A unified framework should assess risks and guide decision-making processes for enhancing system resilience. Organizations need to champion continuous learning and adaptive strategies in light of the fluid nature of process safety and process security risks. This commitment can manifest in routine safety audits, meticulous incident investigations, and periodic revisions of risk assessment frameworks, ensuring their relevance and efficacy.

There is a pressing need to champion further research to refine system-based semi-quantitative techniques and their seamless integration into a cohesive risk assessment framework. Such endeavors will arm the process industry with cutting-edge tools and strategies, fortifying their defenses against process safety, process security, and resilience challenges.

Lastly, the crafting and execution of effective risk assessment frameworks mandate the active participation of all stakeholders, spanning from frontline operators to top management. Their collective insights, experiences, and expertise are invaluable, offering a richer understanding of risks and paving the way for more potent mitigation strategies. By implementing these insights and recommendations, the CPI can effectively address process safety, process security, and resilience, setting the stage for operations that are not only safer but also more secure and resilient.

CRediT authorship contribution statement

Muhammad Shah Ab Rahim: Conceptualization, Data curation, Formal analysis, Methodology, Validation, Visualization, Writing – original draft. **Genserik Reniers:** Conceptualization, Supervision, Writing – review & editing. **Ming Yang:** Conceptualization, Supervision, Validation, Writing – review & editing. **Shailendra Bajpai:** 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

Data will be made available on request.

Acknowledgements

The authors thankfully acknowledge the financial support provided by the Public Service Department Malaysia under the Federal Training Prize 2022 with reference number JPA(1)830227015745.

Appendix A. Analysis of type, techniques, and stage of assessment as described in the literature

No.	Reference **(Chronological ordered)**	Techniques/Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res
1	Bartolozzi et al. (2000)	Hazards and operability analysis (HAZOP) support tool	QL		x			x		
2	Venkatasubramanian et al. (2000)	HAZOP-expert tool	SQ		x					
3	(F. I. Khan and Abbasi, 2001)	Quantitative domino effect analysis	QN		x		x	x	x	
4	(F. I. Khan et al., 2001)	Computer automated tool for risk assessment	SQ		x		x	x	x	
5	Baybutt (2002)	Matrix-based threat and process vulnerability analysis	QL	N		x	x	x	x	

(*continued on next page*)

(*continued*)

No.	Reference **(Chronological ordered)**	Techniques/Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res
6	Caputo et al. (2002)	Fault tree analysis (FTA)	SQ		x		x	x	x	
7	Jaeger (2002)	Checklist-based vulnerability assessment methodology	QL			x	x	x	x	
8	(F. I. Khan et al., 2002)	Probabilistic FTA	QN		x		x	x	x	
9	Kim et al. (2003)	Event tree analysis (ETA), Consequence analysis	SQ		x		x	x	x	
10	Krishna et al. (2003)	Quantitative FTA	QN		x		x	x	x	
11	Lemley et al. (2003)	Matrix-based security risk analysis	SQ	N						
12	Dunbobbin et al. (2004)	Checklist-based security vulnerability assessment	QL	N		x	x	x	x	
13	(J. N. S. Fang et al., 2004)	Quantitative value-at-risk (VAR)	QN		x		x	x	x	
14	Moorel (2004)	Checklist-based security vulnerability assessment	QL	N		x	x		x	
15	Renshaw (2004)	Checklist, Quantitative Risk Assessment (QRA)	SQ		x		x	x	x	
16	Bajpai and Gupta (2005)	Matrix-based Security Risk Factor Table (SRFT)	QL			x	x	x	x	
17	Moore (2006)	Matrix-based Security Vulnerability Assessment (SVA)	QL			x	x		x	
18	Bajpai and Gupta (2007)	SRFT, Expert judgement	QL			x		x	x	
19	Ramzan et al. (2007)	Extended HAZOP, ETA, Risk Matrix	SQ		x		x	x	x	
20	(G. L. L. Reniers et al., 2008)	Quantitative domino security risk assessment	QN			x		x		
21	Bajpai et al. (2010)	SRFT, Expert judgement, Fuzzy logic	SQ			x		x	x	
22	Wasileski and Henselwood (2011)	LOPA	SQ		x		x	x	x	
23	Kleindorfer et al. (2012)	Potential safety loss (near-miss) analysis	SQ		x		x	x	x	
24	Markowski (2012)	Fuzzy LOPA	SQ		x		x	x	x	
25	Podofillini and Dang (2012)	Monte Carlo probabilistic safety assessment	SQ		x		x	x	x	
26	Ávila et al. (2013)	Social HAZOP	QL		x			x		
27	Myers (2013)	LOPA-based human performance	SQ		x		x			
28	Aneziris et al. (2014)	QRA	QN		x		x	x	x	
29	Demichela and Camuncoli (2014)	Extended HAZOP, dynamic ETA	SQ		x		x	x	x	
30	Roy et al. (2014)	BN-based risk and reliability assessment	QN	N	x		x	x	x	
31	Baksh et al. (2015)	BN-based predictive accident modeling	QN		x		x	x	x	
32	Roy et al. (2015)	Dynamic BN-based, ETA	SQ				x	x	x	
33	Wang et al. (2016)	Dynamic quantitative operational risk assessment	QN				x	x	x	
34	Adedigba et al. (2017)	Artificial neural network (ANN), FTA, sequential accident model	SQ		x		x	x	x	
35	Aneziris et al. (2017)	HAZOP, FTA and Bowtie	SQ		x		x	x	x	
36	Argenti et al. (2017)	Quantitative SVA, Expert judgement	QN			x	x			
37	Castillo-Borja et al. (2017)	Monte Carlo-based Safety Resilience Index	QN					x		x
38	Chastain et al. (2017)	HAZOP, LOPA, Failure Mode and Effects Analysis (FMEA) Human Reliability Analysis (HRA)	SQ		x		x	x	x	
39	Kanes et al. (2017)	BN, Bowtie	QN		x		x	x	x	
40	Adedigba et al. (2018)	ETA, BN, modified inverted normal loss function	SQ		x		x	x	x	
41	Dakkoune et al. (2018)	Risk Matrix	SQ		x		x	x	x	
42	Guo et al. (2018)	Revised bow-tie with copula function and Monte Carlo simulation	SQ		x		x	x	x	
44	Hu et al. (2018)	Simplified QRA	QN		x		x	x	x	
45	Jain, Pasman, Waldram, Pistikopoulos, et al. (2018a)	Process resilience analysis framework (PRAF)	SQ		x		x	x	x	x
46	Jain, Rogers, Pasman, Keim, et al. (2018c)	HAZOP, Resilience-based integrated process systems hazard analysis (RIPSHA)	SQ		x		x	x	x	x
47	Casson Moreno et al. (2019)	Bowtie and Consequence-based QRA	SQ		x		x	x	x	
48	Guo et al. (2019)	BN-based Copula function	QN		x		x	x	x	
49	Kamil et al. (2019)	Petri-net based dynamic domino effects risk assessment	SQ		x		x	x	x	
50	(J. Zhou et al., 2019)	Petri-net based attack tree analysis	QN			x	x	x	x	
51	Jain et al. (2019)	PRAF with Bayesian analysis	QN		x		x	x	x	x
52	Jain et al. (2019)	PRAF with Bayesian regression	QN		x		x	x	x	x
53	Janošovský et al. (2019)	HAZOP, Aspen simulation	SQ		x			x		
54	Marhavilas et al. (2019)	HAZOP, Risk Matrix, Analytical Hierarchy Process (AHP)	SQ		x		x	x	x	
55	Song et al. (2019)	Dynamic BN-based Monte Carlo simulation, FTA	QN		x	x	x	x	x	
56	Sultana et al. (2019)	System-Theoretic Accident Model and Processes (STAMP)	SQ		x			x	x	x
57	Yousefi et al. (2019)	FRAM, STAMP, AcciMap	SQ		x			x	x	x
58	Zhang et al. (2019)	QRA, Complete accident scenario set (CASS) and Computational fluid dynamics (CFD)	QN		x		x	x	x	
59	(B et al., 2020)	Dynamic BN-based, Bowtie	QN		x		x	x	x	
60	Bjørnsen et al. (2020)	FRAM, Strength of Knowledge (SoK)	SQ		x			x	x	x
61	(F. Chen et al., 2020)	Dynamic BN-based ETA and Monte Carlo simulation	QN		x		x	x	x	
62	(H. Pasman et al., 2020b)	PRAF, RIPSHA	SQ	N	x		x	x	x	x
63	(J.-Y. Choi and Byeon, 2020)	HAZOP, Safety Integrity Level (SIL)	SQ		x		x	x	x	
64	Marhavilas et al. (2020)	HAZOP, Risk Matrix, AHP	SQ		x		x	x	x	
65	Sano et al. (2020)	Dow's Fire and Explosion Index (DFEI), FTA, Process Safety Metrics, Cost-benefit analysis (CBA)	QN		x		x	x	x	
66	Tong et al. (2020)	Dynamic BN, Markov Chain analysis	QN		x		x	x	x	x
67	Vairo et al. (2020)	Dynamic BN-based and Markov Chain Monte Carlo	QN		x		x	x	x	x
68	(Y. Fang et al., 2020)	ETA-based, Aspen simulation	QN		x		x	x	x	
69	Vaughen et al. (2020)	LOPA, Consequence modelling, Risk Matrix	SQ		x		x	x	x	
70	Benson et al. (2021)	SIL	SQ	N	x		x	x	x	
71	(C. Chen et al., 2021)	Dynamic Monte carlo simulation, TNT explosion model, Probit model, Fire escalation model	QN		x		x	x	x	x

(*continued on next page*)

(*continued*)

No.	Reference **(Chronological ordered)**	Techniques/Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res
72	Cong et al. (2021)	HAZOP, LOPA, Dow's Fire and Explosion Index (DFEI)	SQ		x		x	x	x	
73	Jianxing et al. (2021)	Risk Matrix-based with fuzzy cloud model	SQ				x	x	x	
74	Iaiani et al. (2021)	Correspondence Analysis (CA), Root Cause Analysis (RCA)	SQ			x		x	x	
75	Menezes et al. (2021)	Functional Resonance Analysis Method (FRAM), Performance Shaping Factors (PSF)	QL		x			x	x	x
76	Penelas and Pires (2021)	HAZOP, Risk Matrix	QL		x			x	x	
77	Schmitz et al. (2021)	Bow-tie, Phast simulation	SQ		x			x		
78	Zarei et al. (2021)	Multicriteria decision-making (MCDM), AHP-VIKOR, Fuzzy set theory (FST)	SQ					x		x
79	Zinetullina et al. (2021)	Dynamic BN, FRAM, Aspen HYSIS	SQ		x		x	x	x	x
80	Amin et al. (2022)	BN-based integrated process safety and security analysis	QN		x	x	x	x	x	
81	Eskandarzade et al. (2022)	API Risk Based Inspection Methodology, improved Kent Muhlbauer method	SQ				x	x	x	
82	Ghasemi et al. (2022)	Fuzzy BN, Human Factors Analysis and Classification System (HFACS)	SQ		x		x	x	x	
83	He et al. (2022)	BN-based, Fuzzy measure and Choquet integral	QN		x		x	x	x	
84	Moreno et al. (2022)	Probabilistic SVA, ETA, FTA, Human reliability analysis (HRA)	QN		x	x	x	x	x	
85	(S. Zhou et al., 2022)	STAMP, Computational fluid dynamics (CFD), Convolutional neural network (CNN)	SQ		x		x	x	x	x
86	Santana et al. (2022)	Bowtie, Python fuzzy sets, Takagi–Sugeno inference	SQ		x		x	x	x	
87	Sivaraman et al. (2022)	FTA, Artificial Neural Network (ANN), human error assessment and reduction technique (HEART)	SQ		x		x	x	x	
88	Sun et al. (2022)	Dynamic BN, FRAM	QN					x		x
89	Ylönen et al. (2022)	FTA, ETA, HAZOP, Content Analysis	SQ		x	x	x	x	x	

Notes:

Type refers to the nature of the method:
QL = Qualitative
QN = Quantitative
SQ = Semi-quantitative

Data?
N=No empirical or simulation data presented in the study

Stage of Assessment as presented in the study:
Safe. HI = Process safety-related hazard identification
Sec. HI = Process security-related hazard identification
LA = Likelihood and/or vulnerability analysis
CA = Consequence of event analysis
RC = Overall risk calculation
Res. = Resilience assessment

References

Adedigba, S.A., Khan, F., Yang, M., 2017. Dynamic failure analysis of process systems using neural networks. Process Saf. Environ. Protect. 111, 529–543. https://doi.org/10.1016/j.psep.2017.08.005.

Adedigba, S.A., Khan, F., Yang, M., 2018. An integrated approach for dynamic economic risk assessment of process systems. Process Saf. Environ. Protect. 116, 312–323. https://doi.org/10.1016/j.psep.2018.01.013.

American Chemistry Council, 2022. Guide to the Business of Chemistry, p. 2022.

Amin, Md T., Khan, F., Halim, S.Z., Pistikopoulos, S., 2022. A holistic framework for process safety and security analysis. Comput. Chem. Eng. 165 https://doi.org/10.1016/j.compchemeng.2022.107963.

Amundrud, Ø., Aven, T., Flage, R., 2017. How the definition of security risk can be made compatible with safety definitions. Proc. Inst. Mech. Eng. O J. Risk Reliab. 231 (3), 286–294. https://doi.org/10.1177/1748006X17699145.

Amyotte, P.R., Berger, S., Edwards, D.W., Gupta, J.P., Hendershot, D.C., Khan, F.I., Mannan, M.S., Willey, R.J., 2016. Why major accidents are still occurring. Current Opinion in Chemical Engineering 14, 1–8. https://doi.org/10.1016/j.coche.2016.07.003.

Aneziris, O.N., Papazoglou, I.A., Konstantinidou, M., Nivolianitou, Z., 2014. Integrated risk assessment for LNG terminals. J. Loss Prev. Process. Ind. 28, 23–35. https://doi.org/10.1016/j.jlp.2013.07.014.

Aneziris, O.N., Nivolianitou, Z., Konstandinidou, M., Mavridis, G., Plot, E., 2017. A Total Safety Management framework in case of a major hazards plant producing pesticides. Saf. Sci. 100, 183–194. https://doi.org/10.1016/j.ssci.2017.03.021.

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. https://doi.org/10.1016/j.ssci.2016.11.022.

Aven, T., 2007. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab. Eng. Syst. Saf. 92 (6), 745–754. https://doi.org/10.1016/j.ress.2006.03.008.

Aven, T., Kristensen, V., 2005. Perspectives on risk: review and discussion of the basis for establishing a unified and holistic approach. Reliab. Eng. Syst. Saf. 90 (Issue 1), 1–14. https://doi.org/10.1016/j.ress.2004.10.008.

Ávila, S.F., Pessoa, F.L.P., Andrade, J.C.S., 2013. Social HAZOP at an oil refinery. Process Saf. Prog. 32 (1), 17–21. https://doi.org/10.1002/prs.11552.

B, B., George, P., Renjith, V.R., Kurian, A.J., 2020. Application of dynamic risk analysis in offshore drilling processes. J. Loss Prev. Process. Ind. 68 https://doi.org/10.1016/j.jlp.2020.104326.

Bajpai, S., Gupta, J.P., 2005. Site security for chemical process industries. J. Loss Prev. Process. Ind. 18 (4–6), 301–309. https://doi.org/10.1016/j.jlp.2005.06.011.

Bajpai, S., Gupta, J.P., 2007. Terror-proofing chemical process industries. Process Saf. Environ. Protect. 85 (6 B), 559–565. https://doi.org/10.1205/psep06046.

Bajpai, S., Sachdeva, A., Gupta, J.P., 2010. Security risk assessment: applying the concepts of fuzzy logic. J. Hazard Mater. 173 (1–3), 258–264. https://doi.org/10.1016/j.jhazmat.2009.08.078.

Baksh, A.-A., Khan, F., Gadag, V., Ferdous, R., 2015. Network based approach for predictive accident modelling. Saf. Sci. 80, 274–287. https://doi.org/10.1016/j.ssci.2015.08.003.

Bartolozzi, V., Castiglione, L., Picciotto, A., Galluzzo, M., 2000. Qualitative models of equipment units and their use in automatic HAZOP analysis. Reliab. Eng. Syst. Saf. 70 (1), 49–57. https://doi.org/10.1016/S0951-8320(00)00042-9.

Baybutt, P., 2002. Assessing risks from threats to process plants: threat and vulnerability analysis. Process Saf. Prog. 21 (4), 269–275. https://doi.org/10.1002/prs.680210403.

Baybutt, P., 2017. Issues for security risk assessment in the process industries. J. Loss Prev. Process. Ind. 49, 509–518. https://doi.org/10.1016/j.jlp.2017.05.023.

Benson, C., Argyropoulos, C.D., Dimopoulos, C., Mikellidou, C.V., Boustras, G., 2021. Safety and risk analysis in digitalized process operations warning of possible deviating conditions in the process environment. Process Saf. Environ. Protect. 149, 750–757. https://doi.org/10.1016/j.psep.2021.02.0390957-5820/.

Bjørnsen, K., Jensen, A., Aven, T., 2020. Using qualitative types of risk assessments in conjunction with FRAM to strengthen the resilience of systems. J. Risk Res. 23 (2), 153–166. https://doi.org/10.1080/13669877.2018.1517382.

Cameron, I., Mannan, S., Nemeth, E., Park, S., Pasman, H., Rogers, W., Seligmann, B., 2017. Process hazard analysis, hazard identification and scenario definition: are the conventional tools sufficient, or should and can we do much better? Process Saf. Environ. Protect. 110, 53–70. https://doi.org/10.1016/j.psep.2017.01.025.

Caputo, A.C., Pelagagge, P.M., Tartaglia, R., 2002. Safety management in a hazardous experimental environment: the Borexino case. Process Saf. Prog. 21 (1), 55–66. https://doi.org/10.1002/prs.680210109.

Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process Saf. Environ. Protect. 116, 621–631. https://doi.org/10.1016/j.psep.2018.03.026.

Casson Moreno, V., Garbetti, A.L., Leveneur, S., Antonioni, G., 2019. A consequences-based approach for the selection of relevant accident scenarios in emerging technologies. Saf. Sci. 112, 142–151. https://doi.org/10.1016/j.ssci.2018.10.024.
Castillo-Borja, F., Vázquez-Román, R., Quiroz-Pérez, E., Díaz-Ovalle, C., Sam Mannan, M., 2017. A resilience index for process safety analysis. J. Loss Prev. Process. Ind. 50, 184–189. https://doi.org/10.1016/j.jlp.2017.06.017.
CCPS, 2003. Center for Chemical Process Safety (CCPS) Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, first ed. John Wiley & Sons, Inc.
Chastain, J.W., Delanoy, P., Devlin, C., Mueller, T., Study, K., 2017. Beyond HAZOP and LOPA: four different company approaches. Process Saf. Prog. 36 (1), 38–53. https://doi.org/10.1002/prs.11831.
Chen, F., Wang, C., Wang, J., Zhi, Y., Wang, Z., 2020. Risk assessment of chemical process considering dynamic probability of near misses based on Bayesian theory and event tree analysis. J. Loss Prev. Process. Ind. 68 https://doi.org/10.1016/j.jlp.2020.104280.
Chen, C., Yang, M., Reniers, G., 2021. A dynamic stochastic methodology for quantifying HAZMAT storage resilience. Reliab. Eng. Syst. Saf. 215 https://doi.org/10.1016/j.ress.2021.107909.
Chen, C., Li, J., Zhao, Y., Goerlandt, F., Reniers, G., Yiliu, L., 2023. Resilience assessment and management: a review on contributions on process safety and environmental protection. Process Saf. Environ. Protect. 170, 1039–1051. https://doi.org/10.1016/j.psep.2022.12.072.
Choi, J.Y., Byeon, S.H., 2020. Hazop methodology based on the health, safety, and environment engineering. Int. J. Environ. Res. Publ. Health 17 (9). https://doi.org/10.3390/ijerph17093236.
Cong, G., Lu, D., Liu, M., Wang, Q., Yu, W., 2021. A new semi-quantitative process safety assessment method and its application for Fluorochemical industry. Processes 9 (10). https://doi.org/10.3390/pr9101695.
Cox, L.A., 2008. Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. Risk Anal. 28 (6), 1749–1761. https://doi.org/10.1111/j.1539-6924.2008.01142.x.
Dakkoune, A., Vernières-Hassimi, L., Leveneur, S., Lefebvre, D., Estel, L., 2018. Risk analysis of French chemical industry. Saf. Sci. 105, 77–85. https://doi.org/10.1016/j.ssci.2018.02.003.
Demichela, M., Camuncoli, G., 2014. Risk based decision making. Discussion on two methodological milestones. J. Loss Prev. Process. Ind. 28, 101–108. https://doi.org/10.1016/j.jlp.2013.05.010.
Dunbobbin, B.R., Medovich, T.J., Murphy, M.C., Ramsey, A.L., 2004. Security vulnerability assessment in the chemical industry. Process Saf. Prog. 23 (3), 214–220. https://doi.org/10.1002/prs.10037.
Eskandarzade, M., Shahrivar, R., Ratnayake, R.M.C., Bukhari, U.N., 2022. An optimal approach for Semiquantitative risk-based Inspection of pipelines. J. Pipeline Syst. Eng. Pract. 13 (3) https://doi.org/10.1061/(ASCE)PS.1949-1204.0000653.
Fang, J.N.S., Ford, D.M., Mannan, M.S., 2004. Making the business case for process safety using value-at-risk concepts. J. Hazard Mater. 115 (1–3), 17–26. https://doi.org/10.1016/j.jhazmat.2004.06.004.
Flourish Studio. Flourish: Data Visualization & Storytelling. Retrieved from. https://app.flourish.studio/projects.
Fang, Y., Rasel, M.A.K., Richmond, P.C., 2020. Consequence risk analysis using operating procedure event trees and dynamic simulation. J. Loss Prev. Process. Ind. 67 https://doi.org/10.1016/j.jlp.2020.104235.
Ghasemi, F., Gholamizadeh, K., Farjadnia, A., Sedighizadeh, A., Kalatpour, O., 2022. Human and organizational failures analysis in process industries using FBN-HFACS model: learning from a toxic gas leakage accident. J. Loss Prev. Process. Ind. 78 https://doi.org/10.1016/j.jlp.2022.104823.
Guo, C., Khan, F., Imtiaz, S., 2018. Risk assessment of process system considering dependencies. J. Loss Prev. Process. Ind. 55, 204–212. https://doi.org/10.1016/j.jlp.2018.06.014.
Guo, C., Khan, F., Imtiaz, S., 2019. Copula-based Bayesian network model for process system risk assessment. Process Saf. Environ. Protect. 123, 317–326. https://doi.org/10.1016/j.psep.2019.01.022.
He, Z., Fu, M., Weng, W., 2022. A non-linear risk assessment method for chemical clusters based on fuzzy measure and Choquet integral. J. Loss Prev. Process. Ind. 77 https://doi.org/10.1016/j.jlp.2022.104778.
Hickford, A.J., Blainey, S.P., Ortega Hortelano, A., Pant, R., 2018. Resilience engineering: theory and practice in interdependent infrastructure systems. Environment Systems and Decisions 38 (3), 278–291. https://doi.org/10.1007/s10669-018-9707-4.
Hollnagel, E., Woods, D.D., Leveson, N., 2012. Resilience engineering: concepts and precepts. In: Resilience Engineering: Concepts and Precepts. Ashgate Publishing Ltd. https://doi.org/10.1136/qshc.2006.018390.
Hosseini, S., Barker, K., Ramirez-Marquez, J.E., 2016. A review of definitions and measures of system resilience. Reliab. Eng. Syst. Saf. 145, 47–61. https://doi.org/10.1016/j.ress.2015.08.006.
Hu, X., Wu, Z., Hedlund, F.H., Pedersen, J.B., Wang, R., Duo, Y., Sin, G., 2018. Land-Use planning risk estimates for a chemical industrial park in China - a longitudinal study. Process Saf. Prog. 37 (2), 124–133. https://doi.org/10.1002/prs.11972.
Iaiani, M., Casson Moreno, V., Reniers, G., Tugnoli, A., Cozzani, V., 2021. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab. Eng. Syst. Saf. 212 https://doi.org/10.1016/j.ress.2021.107593.
Jaeger, C.D., 2002. Vulnerability assessment methodology for chemical facilities (VAM-CF). Chem. Health Saf. 9 (6), 15–19. https://doi.org/10.1016/S1074-9098(02)00389-1.
Jain, P., Pasman, H.J., Waldram, S.P., Rogers, W.J., Mannan, M.S., 2017. Did we learn about risk control since Seveso? Yes, we surely did, but is it enough? An historical brief and problem analysis. J. Loss Prev. Process. Ind. 49, 5–17. https://doi.org/10.1016/j.jlp.2016.09.023.
Jain, P., Pasman, H.J., Waldram, S., Pistikopoulos, E.N., Mannan, M.S., 2018a. Process Resilience Analysis Framework (PRAF): a systems approach for improved risk and safety management. J. Loss Prev. Process. Ind. 53, 61–73. https://doi.org/10.1016/j.jlp.2017.08.006.
Jain, P., Pasman, H.J., Waldram, S., Pistikopoulos, E.N., Mannan, M.S., 2018b. Process Resilience Analysis Framework (PRAF): a systems approach for improved risk and safety management. J. Loss Prev. Process. Ind. 53 https://doi.org/10.1016/j.jlp.2017.08.006.
Jain, P., Rogers, W.J., Pasman, H.J., Keim, K.K., Mannan, M.S., 2018c. A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part I plant system layer. Process Saf. Environ. Protect. 116, 92–105. https://doi.org/10.1016/j.psep.2018.01.016.
Jain, P., Diangelakis, N.A., Pistikopoulos, E.N., Mannan, M.S., 2019a. Process resilience based upset events prediction analysis: application to a batch reactor. J. Loss Prev. Process. Ind. 62 https://doi.org/10.1016/j.jlp.2019.103957.
Jain, P., Pistikopoulos, E.N., Mannan, M.S., 2019b. Process resilience analysis based data-driven maintenance optimization: application to cooling tower operations. Comput. Chem. Eng. 121, 27–45. https://doi.org/10.1016/j.compchemeng.2018.10.019.
Janošovský, J., Danko, M., Labovský, J., 2019. Software approach to simulation-based hazard identification of complex industrial processes. Comput. Chem. Eng. 122, 66–79. https://doi.org/10.1016/j.compchemeng.2018.05.021.
JCR, 2023. In: Journal Citation Reports. https://jcr.clarivate.com.
Jianxing, Y., Haicheng, C., Shibo, W., Haizhao, F., 2021. A novel risk matrix approach based on cloud model for risk assessment under uncertainty. IEEE Access 9, 27884–27896. https://doi.org/10.1109/ACCESS.2021.3058392.
Kamil, M.Z., Taleb-Berrouane, M., Khan, F., Ahmed, S., 2019. Dynamic domino effect risk assessment using Petri-nets. Process Saf. Environ. Protect. 124, 308–316. https://doi.org/10.1016/j.psep.2019.02.019.
Kanes, R., Ramirez Marengo, M.C., Abdel-Moati, H., Cranefield, J., Véchot, L., 2017. Developing a framework for dynamic risk assessment using Bayesian networks and reliability data. J. Loss Prev. Process. Ind. 50, 142–153. https://doi.org/10.1016/j.jlp.2017.09.011.
Khan, F.I., Abbasi, S.A., 2001. An assessment of the likehood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. J. Loss Prev. Process. Ind. 14 (4), 283–306. https://doi.org/10.1016/S0950-4230(00)00048-6.
Khan, F.I., Iqbal, A., Abbasi, S.A., 2001. Rapid risk assessment of a fertilizer industry using recently developed computer-automated tool TORAP. J. Loss Prev. Process. Ind. 14 (5), 413–427. https://doi.org/10.1016/S0950-4230(00)00055-3.
Khan, F.I., Sadiq, R., Husain, T., 2002. Risk-based process safety assessment and control measures design for offshore process facilities. J. Hazard Mater. 94 (1), 1–36. https://doi.org/10.1016/S0304-3894(02)00004-3.
Khan, F., Rathnayaka, S., Ahmed, S., 2015. Methods and models in process safety and risk management: past, present and future. Process Saf. Environ. Protect. 98, 116–147. https://doi.org/10.1016/j.psep.2015.07.005.
Kim, K.H., Shin, D., Yoon, E.S., 2003. Risk analysis using automatically synthesized robust accident scenarios and consequence assessment for chemical processes: process partition and consequence analysis approach. Kor. J. Chem. Eng. 20 (6), 992–999. https://doi.org/10.1007/BF02706927.
Kleindorfer, P., Oktem, U.G., Pariyani, A., Seider, W.D., 2012. Assessment of catastrophe risk and potential losses in industry. Comput. Chem. Eng. 47, 85–96. https://doi.org/10.1016/j.compchemeng.2012.06.033.
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. https://doi.org/10.1016/J.RESS.2015.02.008.
Krishna, K., Wang, Y.J., Saraf, S.R., Rogers, W.J., Baldwin, J.T., Gupta, J.P., Mannan, M.S., 2003. Hydroxylamine production: will a QRA help you decide? Reliab. Eng. Syst. Saf. 81 (2), 215–224. https://doi.org/10.1016/S0951-8320(03)00115-7.
Landucci, G., Khakzad, N., Genserik, R., 2020. Physical Security in the Process Industry - Theory with Applications, first ed. Elsevier B.V. https://doi.org/10.1016/C2017-0-00539-6.
Lemley, J.R., Fthenakis, V.M., Moskowitz, P.D., 2003. Security risk analysis for chemical process facilities. Process Saf. Prog. 22 (3), 153–162. https://doi.org/10.1002/prs.680220304.
Logan, T.M.L., Aven, T., Guikema, S.D., Flage, R., 2022. Risk science offers an integrated approach to resilience. Nat. Sustain. 5 (Issue 9), 741–748. https://doi.org/10.1038/s41893-022-00893-w. Nature Research.
Marhavilas, P.K., Koulouriotis, D., Gemeni, V., 2011. Risk analysis and assessment methodologies in the work sites: on a review, classification and comparative study of the scientific literature of the period 2000-2009. J. Loss Prev. Process. Ind. 24 (Issue 5), 477–523. https://doi.org/10.1016/j.jlp.2011.03.004.
Marhavilas, P.K., Filippidis, M., Koulinas, G.K., Koulouriotis, D.E., 2019. The integration of HAZOP study with risk-matrix and the analytical-hierarchy process for identifying critical control-points and prioritizing risks in industry – a case study. J. Loss Prev. Process. Ind. 62 https://doi.org/10.1016/j.jlp.2019.103981.
Marhavilas, P.K., Filippidis, M., Koulinas, G.K., Koulouriotis, D.E., 2020. A HAZOP with MCDM based risk-assessment approach: focusing on the deviations with economic/health/environmental impacts in a process industry. Sustainability 12 (3). https://doi.org/10.3390/su12030993.
Markowski, A.S., 2012. A review of layer of protection analysis techniques for oil and gas industry. Int. J. Oil Gas Coal Technol. 5 (1), 66–79. https://doi.org/10.1504/IJOGCT.2012.044178.

Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2019. A Comparative Analysis of Security Risk Assessment Methodologies for the Chemical Industry, vol. 191. Reliability Engineering and System Safety. https://doi.org/10.1016/j.ress.2018.03.001.

Menezes, M.L.A., Haddad, A.N., Nascimento, M.L.F., 2021. Functional resonance analysis method and human performance factors identifying critical functions in chemical process safety. IEEE Access 9, 168368–168382. https://doi.org/10.1109/ACCESS.2021.3135747.

Meyer, T., Reniers, G.L.L., 2022. Engineering Risk Management, third ed. De Gruyter.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., Altman, D., Antes, G., Atkins, D., Barbour, V., Barrowman, N., Berlin, J.A., Clark, J., Clarke, M., Cook, D., D'Amico, R., Deeks, J.J., Devereaux, P.J., Dickersin, K., Egger, M., Ernst, E., et al., 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. PLoS Med. 6 (Issue 7) https://doi.org/10.1371/journal.pmed.1000097.

Moore, D.A., 2006. Application of the API/NPRA SVA methodology to transportation security issues. J. Hazard Mater. 130 (1–2), 107–121. https://doi.org/10.1016/j.jhazmat.2005.07.042.

Moore, D.A., 2013. Security risk assessment methodology for the petroleum and petrochemical industries. J. Loss Prev. Process. Ind. 26 (6), 1685–1689. https://doi.org/10.1016/j.jlp.2013.10.012.

Moorel, D.A., 2004. The new risk paradigm for chemical process security and safety. J. Hazard Mater. 115 (1–3), 175–180. https://doi.org/10.1016/j.jhazmat.2004.08.017.

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, vol. 228. RELIABILITY ENGINEERING & SYSTEM SAFETY. https://doi.org/10.1016/j.ress.2022.108762.

Myers, P.M., 2013. Layer of Protection Analysis - quantifying human performance in initiating events and independent protection layers. J. Loss Prev. Process. Ind. 26 (3), 534–546. https://doi.org/10.1016/j.jlp.2012.07.003.

Necci, A., Cozzani, V., Spadoni, G., Khan, F., 2015. Assessment of domino effect: state of the art and research Needs. Reliab. Eng. Syst. Saf. 143, 3–18. https://doi.org/10.1016/j.ress.2015.05.017.

Pasman, H., Rogers, W., 2015. The bumpy road to better risk control: a Tour d'Horizon of new concepts and ideas. J. Loss Prev. Process. Ind. 35, 366–376. https://doi.org/10.1016/j.jlp.2014.12.003.

Pasman, H.J., Jung, S., Prem, K., Rogers, W.J., Yang, X., 2009. Is risk analysis a useful tool for improving process safety? J. Loss Prev. Process. Ind. 22 (6), 769–777. https://doi.org/10.1016/j.jlp.2009.08.001.

Pasman, H.J., Rogers, W.J., Mannan, M.S., 2018. How can we improve process hazard identification? What can accident investigation methods contribute and what other recent developments? A brief historical survey and a sketch of how to advance. J. Loss Prev. Process. Ind. 55, 80–106. https://doi.org/10.1016/j.jlp.2018.05.018.

Pasman, H., Kottawar, K., Jain, P., 2020a. Resilience of process plant: what, why, and how resilience can improve safety and sustainability. Sustainability 12 (15). https://doi.org/10.3390/su12156152.

Pasman, H., Kottawar, K., Jain, P., 2020b. Resilience of process plant: what, why, and how resilience can improve safety and sustainability. Sustainability 12 (15). https://doi.org/10.3390/su12156152.

Patriarca, R., Di Gravio, G., Costantino, F., 2017. A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems. Saf. Sci. 91, 49–60. https://doi.org/10.1016/j.ssci.2016.07.016.

Penelas, A.J., Pires, J.C.M., 2021. Hazop analysis in terms of safety operations processes for oil production units: a case study. Appl. Sci. 11 (21) https://doi.org/10.3390/app112110210.

Podofillini, L., Dang, V.N., 2012. Conventional and dynamic safety analysis: comparison on a chemical batch reactor. Reliab. Eng. Syst. Saf. 106, 146–159. https://doi.org/10.1016/j.ress.2012.04.010.

Ramzan, N., Compart, F., Witt, W., 2007. Application of extended Hazop and event-tree analysis for investigating operational failures and safety optimization of distillation column unit. Process Saf. Prog. 26 (3), 248–257. https://doi.org/10.1002/prs.10202.

Reniers, G.L.L., Dullaert, W., Audenaert, A., Ale, B.J.M., Soudan, K., 2008. Managing domino effect-related security of industrial areas. J. Loss Prev. Process. Ind. 21 (3), 336–343. https://doi.org/10.1016/j.jlp.2007.06.007.

Reniers, G., Landucci, G., Khakzad, N., 2020. What safety models and principles can be adapted and used in security science? J. Loss Prev. Process. Ind. 64 https://doi.org/10.1016/j.jlp.2020.104068.

Renshaw, F.M., 2004. A major incident prevention program: ten years of experience. Process Saf. Prog. 23 (2), 155–162. https://doi.org/10.1002/prs.10023.

Roy, A., Srivastava, P., Sinha, S., 2014. Risk and reliability assessment in chemical process industries using Bayesian methods. Rev. Chem. Eng. 30 (5), 479–499. https://doi.org/10.1515/revce-2013-0043.

Roy, A., Srivastava, P., Sinha, S., 2015. Dynamic failure assessment of an ammonia storage unit: a case study. Process Saf. Environ. Protect. 94, 385–401. https://doi.org/10.1016/j.psep.2014.09.004.

Sano, K., Koshiba, Y., Ohtani, H., 2020. Risk assessment and risk reduction of an acrylonitrile production plant. J. Loss Prev. Process. Ind. 63 https://doi.org/10.1016/j.jlp.2019.104015.

Santana, R., Vianna, S.S.V., Silva, F.V., 2022. A novel approach in fuzzy bowtie analysis applying Takagi–Sugeno inference for risk assessment in chemical industry. J. Loss Prev. Process. Ind. 80 https://doi.org/10.1016/j.jlp.2022.104892.

Schmitz, P., Reniers, G., Swuste, P., 2021. Determining a realistic ranking of the most dangerous process equipment of the ammonia production process: a practical approach. J. Loss Prev. Process. Ind. 70 https://doi.org/10.1016/j.jlp.2021.104395.

Sivaraman, S., Tauseef, S.M., Siddiqui, N.A., 2022. Investigative and probabilistic perspective of the accidental release of styrene: a case study in Vizag, India. Process Saf. Environ. Protect. 158, 55–69. https://doi.org/10.1016/j.psep.2021.11.034.

Song, G., Khan, F., Yang, M., 2019. Probabilistic assessment of integrated safety and security related abnormal events: a case of chemical plants. Saf. Sci. 113, 115–125. https://doi.org/10.1016/j.ssci.2018.11.004.

SRA, 2018. Society for Risk Analysis (SRA) Glossary.

Sultana, S., Andersen, B.S., Haugen, S., 2019. Identifying safety indicators for safety performance measurement using a system engineering approach. Process Saf. Environ. Protect. 128, 107–120. https://doi.org/10.1016/j.psep.2019.05.047.

Sun, H., Wang, H., Yang, M., Reniers, G., 2022a. A STAMP-based approach to quantitative resilience assessment of chemical process systems. Reliab. Eng. Syst. Saf. 222 https://doi.org/10.1016/j.ress.2022.108397.

Sun, H., Yang, M., Wang, H., 2022b. A virtual experiment for measuring system resilience: a case of chemical process systems. Reliab. Eng. Syst. Saf. 228, 108829 https://doi.org/10.1016/J.RESS.2022.108829.

Tong, Q., Yang, M., Zinetullina, A., 2020. A dynamic bayesian network-based approach to resilience assessment of engineered systems. J. Loss Prev. Process. Ind. 65 https://doi.org/10.1016/j.jlp.2020.104152.

Vairo, T., Reverberi, A.P., Fabiano, B., 2020. From risk assessment to resilience assessment. an application to a hazmat storage plant. Chemical Engineering Transactions 82, 151–156. https://doi.org/10.3303/CET2082026.

Varadharajan, S., Bajpai, S., 2023. Chronicles of security risk assessment in process industries: past, present and future perspectives. J. Loss Prev. Process. Ind. 84 https://doi.org/10.1016/j.jlp.2023.105096.

Vaughen, B.K., Hurban, D.A., First, K., Ness, A., 2020. The risk analysis screening tool: Part I, overview. Process Saf. Prog. 39 (2) https://doi.org/10.1002/prs.12142.

Venkatasubramanian, V., Zhao, J., Viswanathan, S., 2000. Intelligent systems for HAZOP analysis of complex process plants. Comput. Chem. Eng. 24 (9–10), 2291–2302. https://doi.org/10.1016/S0098-1354(00)00573-1.

Villa, V., Paltrinieri, N., Khan, F., Cozzani, V., 2016. Towards dynamic risk analysis: a review of the risk assessment approach and its limitations in the chemical process industry. Saf. Sci. 89, 77–93. https://doi.org/10.1016/j.ssci.2016.06.002.

Wagner, T., Champion, J., 2012. A work process for revalidating LOPAs and other risk analyses. Process Saf. Prog. 31 (2), 122–129. https://doi.org/10.1002/prs.11473.

Wang, H., Khan, F., Ahmed, S., Imtiaz, S., 2016. Dynamic quantitative operational risk assessment of chemical processes. Chem. Eng. Sci. 142, 62–78. https://doi.org/10.1016/j.ces.2015.11.034.

Wasileski, R.F., Henselwood, F., 2011. LOPA onions: peeling back the outer layers. Process Saf. Prog. 30 (2), 122–125. https://doi.org/10.1002/prs.10427.

Yang, M., Sun, H., Geng, S., 2023. On the quantitative resilience assessment of complex engineered systems. Process Saf. Environ. Protect. 174, 941–950. https://doi.org/10.1016/J.PSEP.2023.05.019.

Yarveisy, R., Sun, H., Yang, M., Pasman, H., 2022. Resilience Analysis of Digitalized Process Systems, pp. 591–629. https://doi.org/10.1016/bs.mcps.2022.05.002.

Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Cozzani, V., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Gotcheva, N., Del Prete, E., 2022. Integrated management of safety and security in Seveso sites - sociotechnical perspectives. Saf. Sci. 151 https://doi.org/10.1016/j.ssci.2022.105741.

Yousefi, A., Rodriguez Hernandez, M., Lopez Peña, V., 2019. Systemic accident analysis models: a comparison study between AcciMap, FRAM, and STAMP. Process Saf. Prog. 38 (2) https://doi.org/10.1002/prs.12002.

Zarei, E., Ramavandi, B., Darabi, A.H., Omidvar, M., 2021. A framework for resilience assessment in process systems using a fuzzy hybrid MCDM model. J. Loss Prev. Process. Ind. 69 https://doi.org/10.1016/j.jlp.2020.104375.

Zotero. Your personal research assistant. Retrieved from. https://www.zotero.org/user/login.

Zhang, B., Liu, Y., Qiao, S., 2019. A quantitative individual risk assessment method in process facilities with toxic gas release hazards: a combined scenario set and CFD approach. Process Saf. Prog. 38 (1), 52–60. https://doi.org/10.1002/prs.11979.

Zhou, J., Reniers, G., Zhang, L., 2019. Petri-net based attack time analysis in the context of chemical process security. Comput. Chem. Eng. 130 https://doi.org/10.1016/j.compchemeng.2019.106546.

Zhou, S., Wang, Z., Li, Q., 2022. A conceptual framework integrating numerical simulation with system theory based method for quantitative explosion process hazard analysis. Process Saf. Environ. Protect. 166, 202–211. https://doi.org/10.1016/j.psep.2022.08.003.

Zinetullina, A., Yang, M., Khakzad, N., Golman, B., 2020. Dynamic resilience assessment for process units operating in Arctic environments. Safety in Extreme Environments 2 (1), 113–125. https://doi.org/10.1007/s42797-019-00008-3.

Zinetullina, A., Yang, M., Khakzad, N., Golman, B., Li, X., 2021. Quantitative resilience assessment of chemical process systems using functional resonance analysis method and Dynamic Bayesian network. Reliab. Eng. Syst. Saf. 205 https://doi.org/10.1016/j.ress.2020.107232.