

Article

Integrating Process Safety and Process Security Risk Management: Practitioner Insights for a Resilience-Oriented Framework

Muhammad Shah Ab Rahim ^{1,2,*} , Genserik Reniers ^{1,3,4}, Ming Yang ^{1,5,6}  and Parthiban Siwayanan ⁷ 

- ¹ Safety and Security Science Section, Faculty of Technology, Policy and Management, Delft University of Technology, 2628 BX Delft, The Netherlands; g.l.m.e.reniers@tudelft.nl (G.R.); m.yang-1@tudelft.nl (M.Y.)
- ² Department of Occupational Safety and Health Malaysia, Ministry of Human Resources, Federal Government Administrative Centre, 62530 Putrajaya, Malaysia
- ³ Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, 2000 Antwerp, Belgium
- ⁴ Centre for Economics and Corporate Sustainability (CEDON), KU Leuven, 1000 Brussels, Belgium
- ⁵ Centre of Hydrogen Energy, Institute of Future Energy, Universiti Teknologi Malaysia, UTM Johor Bahru, 81310 Johor Bahru, Malaysia
- ⁶ National Centre of Maritime Engineering and Hydrodynamics, Australian Maritime College, University of Tasmania, Launceston, TAS 7248, Australia
- ⁷ Chemical Engineering Department, Xiamen University Malaysia, 43900 Sepang, Malaysia; parthiban.siwayanan@xmu.edu.my
- * Correspondence: a.r.m.s.binabrahim@tudelft.nl

Abstract: Integrating process safety and process security risk management is increasingly essential for enhancing resilience in the chemical process industry. This study addresses how practitioners perceive the integration of these two domains, identifying key benefits, barriers, and strategies for effective implementation. A mixed-methods approach was applied, combining quantitative survey data from 47 industry professionals with qualitative insights from open-ended responses. The findings highlight significant advantages of integration, such as optimized resource use, reduced operational redundancies, and improved risk management. However, barriers such as knowledge gaps, resource constraints, and communication silos were identified. Respondents emphasized the importance of adopting a resilience-oriented approach involving proactive risk management, continuous improvement, and adaptability in both safety and security practices. Critical enablers for integration include strong leadership, alignment of societal values, cross-disciplinary training, and integrated risk assessment methodologies. Emerging technologies and regulatory alignment were also identified as critical factors in facilitating integration. The study contributes to the theoretical understanding of integrated risk management by supporting resilience engineering and systems theory. It offers actionable strategies for overcoming barriers and leveraging enablers, laying the groundwork for developing a resilience-oriented framework for process safety and process security risk management.

Keywords: process safety; process security; resilience; risk management; chemical process industry; systems theory; practitioners



Academic Editors: Piotr Rybarczyk and Giuseppina Adiletta

Received: 12 November 2024

Revised: 2 January 2025

Accepted: 14 January 2025

Published: 1 February 2025

Citation: Ab Rahim, M.S.; Reniers, G.; Yang, M.; Siwayanan, P. Integrating Process Safety and Process Security Risk Management: Practitioner Insights for a Resilience-Oriented Framework. *Processes* **2025**, *13*, 392. <https://doi.org/10.3390/pr13020392>

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The chemical process industry (CPI) is characterized by complex operations that involve processing chemicals into a wide range of products and materials essential to various sectors, such as petrochemicals, pharmaceuticals, and agriculture. To manage the inherent

risks in such operations, the CPI has historically prioritized safety through the implementation of rigorous process safety management (PSM) systems [1–3]. Process safety focuses on identifying, assessing, and mitigating risks arising from unintentional incidents such as equipment failures, human errors, and operational disruptions, which could lead to catastrophic events, including large hazardous chemical releases, fires, and explosions [4,5]. Established methodologies such as Hazard and Operability studies (HAZOP), fault tree analysis (FTA), and layer of protection analysis (LOPA) have been instrumental in reducing such risks [5,6]. However, while effective, these methodologies often focus on individual hazards and reveal limitations in addressing systemic risks, necessitating more comprehensive frameworks for modern industrial operations [7–10].

On the other hand, process security focuses on protecting industrial facilities from intentional malicious acts, including sabotage, terrorism, and cyber-attacks [11,12]. Despite reports of 373 security-related incidents in industrial facilities [13], process security has received comparatively less attention than process safety [8]. Established methods, such as the vulnerability assessment methodology for chemical facilities (VAM-CF) and the security vulnerability assessment (SVA) method, have been developed to address these risks [14,15]. However, their application remains underutilized compared to process safety assessments, creating gaps in preparedness for intentional threats [8,16].

Traditionally, process safety and process security have been managed separately, creating silos that result in inefficiencies and gaps in addressing their interconnected risks [17–19]. The evolving risk landscape in the CPI—marked by increasing complexity, interconnected systems, and emerging technologies—calls for a more integrated risk management approach that combines both process safety and process security considerations [8,17]. The growing complexity of CPI operations, driven by technological advancements and dynamic processes, introduces new and unforeseen risks that demand comprehensive strategies [5]. Nevertheless, current risk management practices often overlook the interdependencies between safety and security risks, reducing the effectiveness of mitigation efforts [8,17].

The operations of CPI significantly impact both workers and surrounding communities, making societal values a critical factor in shaping risk management strategies. Societal values refer to the collective convictions that guide decisions in striving for a just and safe society [20]. Examples include risk reduction, regulatory compliance, operational efficiency, and environmental stewardship [21]. These values are central to decision-making processes, as they influence the priorities and trade-offs in managing process safety and process security risks. Aligning these values is essential for creating a cohesive and effective integrated risk management framework, yet the literature offers limited insight into how practitioners perceive and balance these values in practice. Addressing this gap is crucial for understanding the underlying drivers behind integrated risk management decisions in the CPI.

Moreover, resilience engineering has emerged as a promising paradigm to address the gaps in traditional risk management approaches [22,23]. Resilience engineering emphasizes the ability of systems to anticipate, adapt, and recover from both unintentional and intentional disruptions, including technical failures, terrorism, and natural hazards [23,24]. Key methodologies, such as the functional resonance analysis method (FRAM) and systems theoretic accident model and processes (STAMP), offer a more holistic perspective on risk management by focusing on system-wide interactions and adaptive capacity [8,24,25]. Incorporating resilience principles enables organizations to enhance their ability to manage both process safety and process security risks within a unified framework.

While several studies have highlighted the importance of integrating safety and security risk assessments to improve system resilience [8,17,24], there remain significant gaps in empirical research on how practitioners perceive, implement, and adapt to integrated

frameworks within the CPI. This study seeks to address these gaps by examining industrial practices, engaging stakeholders in decision-making, gathering insights into practical implementation, and identifying challenges and opportunities for integrating process safety and process security risk management. To achieve this, the following research questions are addressed:

- i. How do practitioners perceive the usefulness and benefits of integrating process safety and process security risk management?
- ii. What are practitioners' awareness and perceptions regarding the resilience-based approach for integration?
- iii. How do practitioners perceive the importance of different societal values in process safety and process security risk management?
- iv. What barriers and enablers exist for integrating process safety and process security risk management, according to practitioners?
- v. What strategies do practitioners propose for effective integration?

This research aims to explore the integration of process safety and process security risk management, leveraging resilience engineering principles to address both unintentional and intentional risks. By assessing the perceptions, awareness, and challenges faced by industrial practitioners, the research identifies critical barriers and enablers while proposing actionable strategies for effective integration. Although the development of a unified framework is beyond the scope of this paper, the findings contribute valuable insights and best practices from the domain of process safety, process security, and resilience engineering. These insights offer knowledge for industry practitioners to enhance their risk management practices and lay the groundwork for future efforts toward a cohesive and integrated framework.

The structure of this paper is as follows: Section 2 presents the research methodology. Section 3 presents the findings, followed by a discussion in Section 4. The paper concludes with Section 5.

2. Methodology

This study adopted a mixed-methods approach, integrating quantitative survey design with qualitative thematic analysis [26–28]. The primary aim was to explore industry practitioners' perceptions and experiences regarding the integration of process safety and process security risk management. The mixed-methods approach was selected to capture broad trends through quantitative data while also gathering contextual insights via qualitative responses, leveraging the strengths of both methods to support the study's exploratory objectives. However, we acknowledge that survey-based qualitative data collection has inherent limitations, such as notably less depth and spontaneity. To address this, in-depth interviews with practitioners have been conducted as part of a broader research effort, focusing on follow-up research questions. These interviews will be presented in a separate publication to enrich the understanding of process safety and process security integration.

The survey instrument was developed based on a systematic literature review by the author [8] and findings by Ylönen et al. (2022) [17]. These studies provided insights into existing practices, challenges, and theoretical frameworks surrounding process safety, process security, and resilience in the CPI. This review informed the formulation of 31 multiple-choice questions designed to assess perceptions and levels of agreement (e.g., Likert scales) alongside six open-ended questions aimed at gathering qualitative insights into barriers, enablers, and strategies for integration.

Before finalizing the survey, a pilot test was conducted with six relevant practitioners and academics, who provided feedback on the clarity, structure, and content of the questions. Their input was incorporated to refine the final version, ensuring that the survey

addressed key industry concerns and that respondents could understand the terminology and concepts. The refinements included simplifying definitions, rephrasing ambiguous questions, and restructuring sections for improved flow.

The survey provided definitions of key concepts, including process safety, process security, resilience, and relevant societal values, such as risk reduction and regulatory compliance, to enhance clarity. These definitions were included at the beginning of the related section to ensure that all participants shared a common understanding of the terms, reducing the risk of misinterpretation. The final survey comprised six sections covering respondent background, current practices, resilience awareness, societal values, barriers, enablers, and strategies for effective integration.

The survey was administered via the Microsoft Forms online platform. Participants were recruited using voluntary responses and snowball sampling methods. This approach was chosen to reach a specialized audience of practitioners within the CPI, leveraging the author's professional network to identify individuals actively involved in process safety and security risk management. Although snowball sampling inherently limits representativeness, efforts were made to include a diverse range of perspectives by targeting professionals across different roles (e.g., regulatory staff, safety and security managers, operational personnel) and geographic locations. This approach aligns with the study's exploratory objectives, prioritizing a breadth of qualitative insights over statistical representativeness. While not fully representative, the sample provided sufficient diversity to capture varied perspectives, supporting the qualitative dimension of the study. The survey was available from 1 February to 31 March 2024, and respondents could complete it anonymously with the option to withdraw at any time.

Quantitative data were analyzed using descriptive statistics to provide insights into respondent demographics and their perceptions of integrated risk management. Likert-scale responses assessed levels of agreement with statements on the perceived usefulness of resilience-based approaches, the integration of process safety and security, and strategies for effective integration. Data were reviewed for completeness, and inconsistent or incomplete responses were excluded. For example, Likert-scale responses were checked for anomalies, such as contradictory answers within the same response set, to ensure consistency. Results were summarized through descriptive statistics and visualized using tables and charts to highlight key trends and patterns.

Qualitative data from the open-ended questions were analyzed using the thematic analysis matrix (TAM) technique adapted from Mohd Zairul, 2021 [26]. The TAM enables the systematic identification and organization of qualitative data through a combination of deductive and inductive coding approaches. Deductive codes are predefined categories based on the existing literature or research objectives, such as resilience capabilities. In contrast, inductive codes are derived directly from the data, representing new or unexpected insights that emerge during analysis.

The process began with open coding, where individual segments of text were labeled with initial codes to capture their meaning. These codes were then grouped into categories representing broader areas of interest, such as societal values or integration strategies. Finally, categories were synthesized into overarching themes that describe the key findings of the study. Emerging themes, specifically those identified through inductive coding, highlighted novel patterns or perspectives that were not initially anticipated.

The research team conducted iterative reviews of the codes and themes to ensure accuracy, consistency, and relevance. Qualitative data analysis software (ATLAS.ti) facilitated transparency and rigor by systematically organizing the data and maintaining traceability to the original responses. These findings were structured and presented using a

thematic analysis matrix, visually illustrating the relationships between codes, categories, and themes.

To ensure transparency and replicability, the survey questionnaire and the anonymized dataset are available through the publicly accessible research repository 4TU.ResearchData at <https://data.4tu.nl/datasets/4522882f-0d76-46ad-b63f-5344964e1fb8>, accessed on 2 January 2025. The anonymized data will be accessible under a CC-BY license, and readers may request additional information from the corresponding author if needed.

This study was approved by the Human Research Ethics Committee of TU Delft on 17 January 2024. Participation was voluntary, and no personally identifiable information was collected. The data were anonymized and analyzed in aggregate form to safeguard privacy. Respondents could optionally provide contact details for follow-up interviews, though this was not mandatory.

3. Results

3.1. Respondent Demographics

As shown in Figure 1, a total of 47 participants responded to the survey, representing a diverse range of sectors, positions, and professional experiences within the chemical process industry (CPI). The respondents were predominantly based in Malaysia (61%, $n = 36$) and the Netherlands (23%, $n = 11$), reflecting the survey's outreach and the authors' networks.

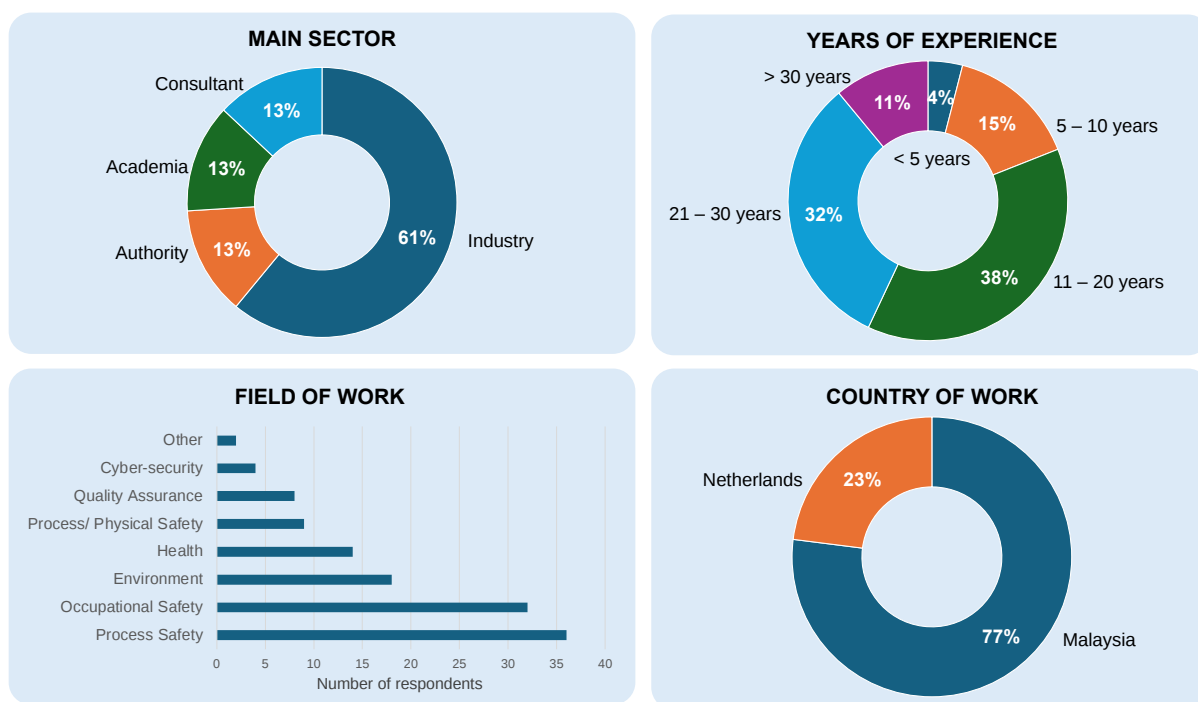


Figure 1. Demographic distributions of respondents ($n = 47$) based on main sectors, years of experience, country of work, and field of work (adapted from [19]).

Respondents were drawn from various sectors of the CPI. The majority were from industry (62%, $n = 29$), followed by consultancy (13%, $n = 6$), authority (13%, $n = 6$), and academia (13%, $n = 6$). This distribution reflects a broad cross-section of stakeholders involved in process safety and security management, offering a range of perspectives from both practical and academic settings.

The participants brought substantial professional experience to the survey, with 81% ($n = 38$) having over 10 years of experience in their respective fields. Specifically, 38%

($n = 18$) reported between 11 and 20 years of experience, 32% ($n = 15$) had 21–30 years of experience, and 11% ($n = 5$) had more than 30 years of experience. This high level of expertise among the respondents ensures that the insights gathered from the survey reflect a depth of knowledge in process safety and security risk management practices.

Furthermore, as summarized in Table 1, a cross-tabulation of country vs. sector indicates that respondents from Malaysia are predominantly engaged in industry (58%, $n = 21$), with smaller proportions involved in authority (17%, $n = 6$), consultancy (14%, $n = 5$), and academia (11%, $n = 4$). Conversely, respondents from the Netherlands were also primarily from industry (73%, $n = 8$) but with a notable presence in academia (18%, $n = 2$), while only one respondent reported working in consultancy.

Table 1. The cross-tabulation demographic of respondents is based on the country of work, main sectors, and years of experience.

Country vs. Sector	Industry	Academia	Authority	Consultancy	
Malaysia	21	4	6	5	
The Netherlands	8	2	0	1	
Country vs. Years of Experience	<5 years	5–10 years	11–20 years	21–30 years	>30 years
Malaysia	2	7	18	9	0
The Netherlands	0	0	0	6	5
Sector vs. Years of Experience	<5 years	5–10 years	11–20 years	21–30 years	>30 years
Industry	1	5	13	7	3
Academia	1	0	1	3	1
Authority	0	2	2	2	0
Consultancy	0	0	2	3	1

A cross-tabulation of country vs. years of experience reveals that respondents from Malaysia had a wider distribution across experience levels. The largest group (50%, $n = 18$) had between 11 and 20 years of experience, followed by 21–30 years (25%, $n = 9$). In contrast, respondents from the Netherlands showed a greater concentration of highly experienced professionals, with 55% ($n = 6$) having 21–30 years of experience and 35% ($n = 5$) having over 30 years.

Regarding sector vs. years of experience, the industry sector had the most significant representation of respondents, with 11–20 years of experience (45%, $n = 13$), followed by those with 21–30 years (24%, $n = 7$). A few participants in industry had over 30 years of experience (10%, $n = 3$), while some had less than 5 years (3%, $n = 1$). In academia, most respondents had between 21 and 30 years ($n = 3$) or more than 30 years of experience ($n = 1$), with very few in the lower experience categories. In authority, the respondents were spread evenly between five and thirty years of experience, while consultancy showed concentration distribution across 11 to 30 years of experience ranges.

3.2. Perception on Integration Usefulness

To assess how practitioners perceive the integration of process safety and process security risk management, respondents were asked whether they consider the integration to be useful. Figure 2 provides a visual representation of the perceived usefulness of integration among respondents by country and sector. The graph shows that 72% ($n = 34$) of respondents found the integration useful, 23% ($n = 11$) were neutral, and 4% ($n = 2$) did not find it useful. The left side of the graph illustrates the overall responses, while the flow links to specific countries and sectors on the right side, helping readers understand the breakdown by group.

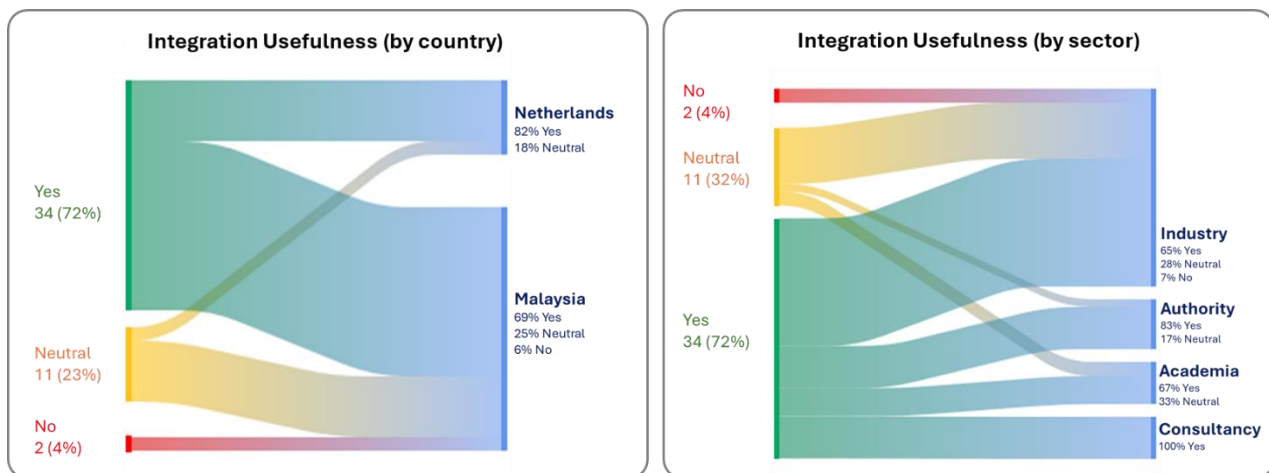


Figure 2. Perceived usefulness for the integration among respondents by country and sector.

Cross-tabulation by country showed similar levels of support between Malaysia and the Netherlands. Among Malaysian respondents, 69% ($n = 25$) indicated that the integration of process safety and process security was beneficial, while 25% ($n = 9$) held neutral views and 6% ($n = 2$) did not find the integration useful. Conversely, respondents from the Netherlands showed a slightly higher level of support, with 82% ($n = 9$) finding the integration useful. In comparison, a smaller proportion (18%, $n = 2$) were neutral, and none of the respondents from the Netherlands indicated that the integration was not useful.

Sectoral analysis revealed further differences. Industry respondents showed strong support, with 66% ($n = 19$) finding integration useful, 28% ($n = 8$) neutral, and 7% ($n = 2$) not finding it useful. In the consultancy sector, all respondents ($n = 6$) found integration useful, while in authority roles, 83% ($n = 5$) found it useful and 17% ($n = 1$) were neutral. Academia showed a more divided view, with 67% ($n = 4$) finding integration useful and 33% ($n = 2$) expressing neutral opinions.

The qualitative responses provided further depth to these quantitative findings, highlighting why respondents found the integration of process safety and process security useful, as summarized in the thematic analysis matrix (Figure 3). Several key themes emerged from the open-ended responses, reflecting a consensus on the interconnectedness of safety and security risks and the importance of a proactive, systematic approach to managing them.

Respondents emphasized the shared nature of risks between process safety and process security. One Malaysian authority figure commented the following: *“In most cases, safety and security risk share the same hazard and effect. The differences would be in terms of caused (intentional vs. unintentional). Therefore, the convergence of these two aspects can strengthen the facility readiness in managing the safety and security threat”*. This view was mirrored by a consultant from Malaysia, who remarked the following: *“Either domain may pose risks to one another. Hence, integrating both domains may eliminate risks between them”*.

In addition to risk mitigation, several respondents discussed the potential for resource optimization through integration. A respondent from the Netherlands in the industry sector emphasized the operational benefits: *“Process safety and process security risk are important to make sure no one gets hurt. Integrating them in our daily operations reduces the risk of incidents or minimizes the impact when incidents do occur”*. This perspective highlights the practical benefits of integration, particularly in minimizing the severity of incidents.

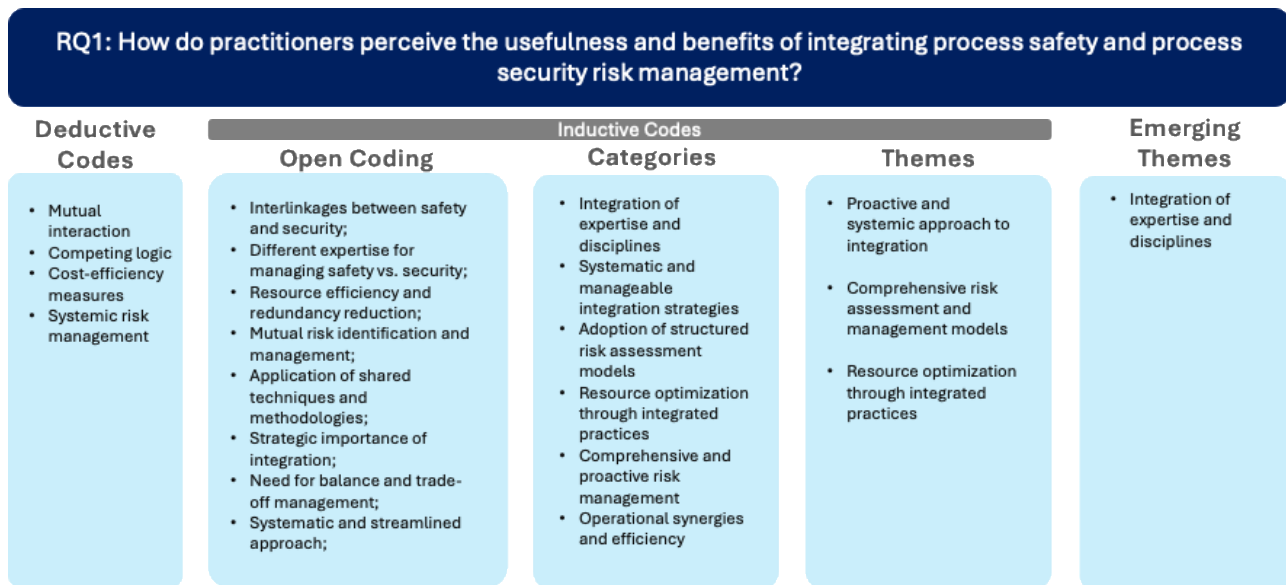


Figure 3. Thematic analysis matrix of practitioners' perception of the usefulness and benefit of integrating process safety and process security risk management.

Moreover, respondents identified the commonality of methodologies between process safety and process security. An academic respondent from the Netherlands noted the following: *"Same risk assessment principles and process steps, e.g., identify, assess, minimize, control"*. This underscores that existing risk management frameworks could be leveraged for both process safety and process security, streamlining the integration efforts.

The combination of the quantitative and qualitative analyses demonstrates a strong shared belief among practitioners in the value of integrating process safety and process security risk management. Quantitatively, most respondents across countries and sectors found integration useful, and these perceptions were enriched by qualitative insights that emphasized the interrelated nature of risks and the efficiency gains from integrated approaches.

The numerical data and the thematic analysis point toward a consensus on the practical and strategic benefits of integration, with respondents calling for systematic approaches, resource optimization, and cross-disciplinary collaboration. These findings suggest that integration is not only viewed as beneficial but also necessary for enhancing overall risk management effectiveness.

3.3. Awareness and Perception on Resilience Concept

To explore how practitioners perceive the resilience-based approach in managing process safety and security risks, respondents were asked to rate their familiarity with the concept and their perceptions of its usefulness (Table 2). The analysis revealed important insights regarding both familiarity and usefulness, as well as how these perceptions vary by country and experience level.

As shown in Table 2, most respondents (70%, $n = 33$) reported being either slightly or moderately familiar with resilience concepts. In comparison, only a tiny portion (6%, $n = 3$) considered themselves very familiar, and none indicated they were extremely familiar. Familiarity varied notably between countries and across different levels of professional experience. Among Malaysian respondents, familiarity levels were more diverse, particularly within the 11–20 years of experience group, where responses ranged from not at all familiar to very familiar. In contrast, Dutch respondents with more than 21 years of experience mostly (91%) described themselves as slightly or moderately familiar, with none reporting very or extremely familiar. These findings suggest that while moderate

familiarity is common, a more profound understanding of resilience concepts is limited, particularly in the Netherlands, where even highly experienced practitioners tend to lack advanced familiarity.

Table 2. Familiarity with the resilience concept by country and years of experience.

Country, Years of Experience	Not at All Familiar	Slightly Familiar	Moderately Familiar	Very Familiar	Extremely Familiar
Malaysia, <5 years	0	0	2	0	0
Malaysia, 5–10 years	3	2	2	0	0
Malaysia, 11–20 years	5	6	5	2	0
Malaysia, 21–30 years	2	5	1	1	0
The Netherlands, 21–30 years	1	2	3	0	0
The Netherlands, >30 years	0	1	4	0	0
Total	11 (23%)	16 (34%)	17 (36%)	3 (6%)	0

In terms of perceived usefulness (Table 3), the majority of respondents (45%, $n = 21$) found resilience concepts to be useful, while 13% ($n = 6$) considered them very useful. Notably, there was variation in how practitioners from different countries and experience levels rated the usefulness of resilience concepts. Among Malaysian respondents, 16 out of 36 participants (61%) rated resilience as either useful or very useful, indicating more substantial overall support for resilience-based approaches. In contrast, among Dutch respondents, only five out of eleven participants (45%) rated resilience concepts as either useful or very useful, reflecting a more mixed perception.

Table 3. Perceived usefulness of resilience concepts by country and years of experience.

Country, Years of Experience	Not Useful	Less Useful	Neutral	Useful	Very Useful
Malaysia, <5 years	0	0	0	2	0
Malaysia, 5–10 years	0	1	2	3	1
Malaysia, 11–20 years	1	1	6	7	3
Malaysia, 21–30 years	0	1	2	5	1
The Netherlands, 21–30 years	0	0	3	3	0
The Netherlands, >30 years	0	1	2	1	1
Total	1 (2%)	4 (8%)	15 (32%)	21 (45%)	6 (13%)

Moreover, Malaysian respondents with less than five years of experience unanimously found resilience concepts useful. However, those with 11–20 years of experience were more divided, with seven respondents finding resilience useful and three rating it as very useful, while six remained neutral. Among Dutch practitioners with more than 21 years of experience, perceptions were also mixed, with four respondents rating resilience as useful and one rating it as very useful. These findings suggest that perceptions of resilience-based approaches vary by experience and national context, with stronger support observed among Malaysian respondents.

Furthermore, the heatmap analysis in Figure 4 provided additional insights into the relationship between familiarity and perceived usefulness. Respondents who were moderately familiar with resilience concepts were the most likely to find them useful or very useful, whereas those with only slight familiarity tended to remain neutral. This suggests that moderate familiarity is sufficient for practitioners to recognize the value of resilience-based approaches. However, the lack of respondents in the “extremely familiar” category and the relatively high number of neutral responses across all familiarity levels indicate that deeper understanding or practical exposure may be needed to appreciate the benefits of resilience-based approaches fully.

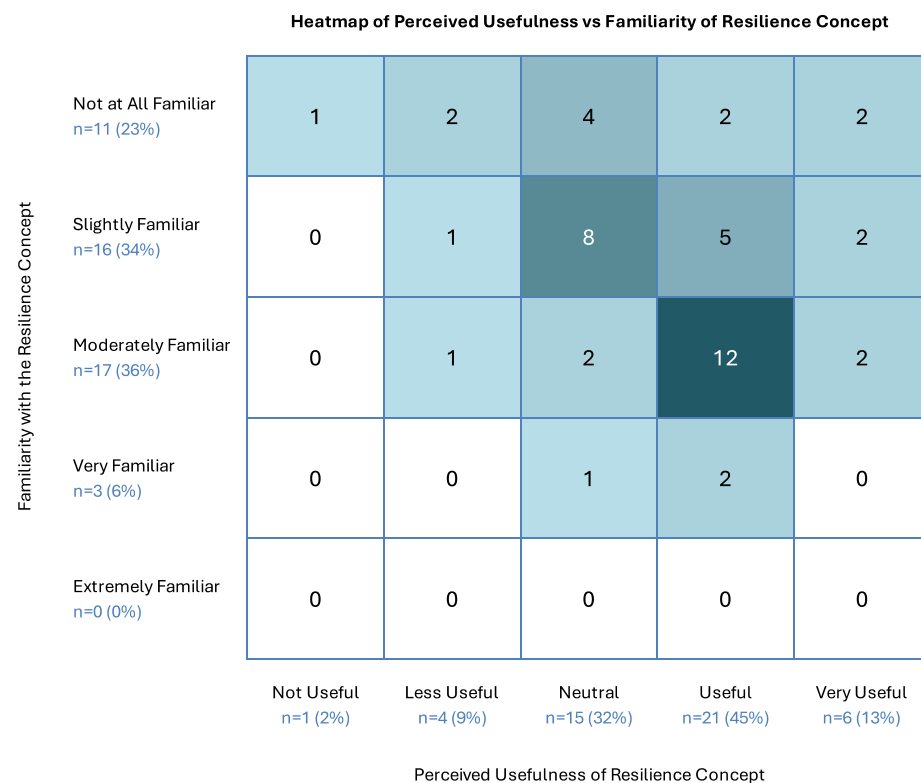


Figure 4. Heatmap of perceived usefulness vs. familiarity on resilience concept among respondents.

We also asked the respondent in an open-ended question to list any resilience-based practices or principles they are aware of. The qualitative responses supported these quantitative findings, revealing several key categories and themes that align with broader resilience frameworks (Figure 5). One key category that emerged was anticipation and proactivity. Respondents emphasized the importance of anticipating risks and taking proactive measures to mitigate them before they escalate. For instance, a consultant from Malaysia highlighted anticipation as a key practice in resilience, stressing the need for the early identification of potential threats. This reflects the proactive stance central to resilience-based approaches, which aim to address risks before they become critical issues.

Another important category was adaptability and system design. Respondents discussed the need for adaptable systems that are capable of handling disruptions and ensuring safety under varying conditions. Practices such as redundancy, diversity, and system reviews were mentioned as vital components of resilience. An academic from the Netherlands cited specific resilience practices such as “*tiered risk assessment, Process Hazard Analyses, and Inherently Safe by Design*”, which underscore the structured and adaptive nature of resilience approaches. These systems are designed to be flexible and able to respond to changes in the operational environment while maintaining safety and security.

Respondents also mentioned the categories of recovery and emergency response. Respondents emphasized the importance of having effective recovery and emergency response mechanisms in place to ensure that operations can continue or recover quickly in the event of an incident. A consultant from Malaysia pointed to business contingency plans as a key resilience practice that allows organizations to bounce back from disruptions. This category also includes practices like emergency response planning and incident sharing, which enable organizations to learn from incidents and enhance their resilience over time.

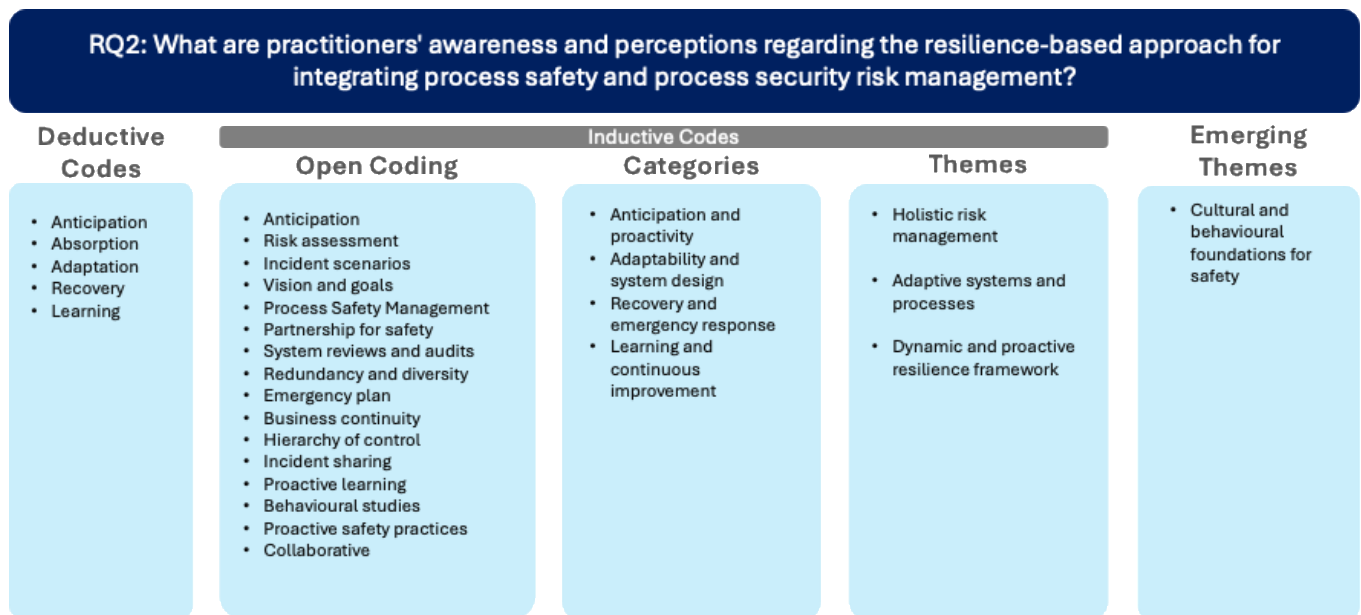


Figure 5. Thematic analysis matrix of practitioners' awareness and perception of the resilience-based approach for integrating process safety and process security risk management.

Respondents also highlighted the significance of learning and continuous improvement. Several emphasized the need to learn from both successful and unsuccessful events to improve safety practices continually. A Malaysian academic mentioned proactive learning from successful tasks, demonstrating how organizations can enhance their resilience through reflection and adaptation. Continuous learning is an integral part of resilience, as it allows organizations to evolve and better manage risks in the future.

Finally, the category of cultural and behavioral foundations for safety emerged as a critical component of resilience-based approaches. Many respondents noted the importance of organizational culture and human behavior in building resilience. An authority figure from Malaysia mentioned behavioral-based studies as essential for understanding and improving human factors in resilience. This highlights that resilience goes beyond technical systems and requires a cultural commitment to safety, collaboration, and proactive behavior within the organization.

From these categories, several broader themes emerged that offer deeper insights into how resilience-based approaches are understood and applied in practice. One key theme is holistic risk management, which draws from the categories of anticipation, adaptability, and learning. Practitioners see resilience as an integral part of a comprehensive risk management framework rather than an isolated strategy. This theme reflects the understanding that resilience-based approaches are embedded within broader efforts to manage risks across the organization.

Another emerging theme is the concept of a dynamic and proactive resilience framework. This theme combines insights from the categories of adaptability and continuous improvement, highlighting that resilience is not a static attribute but rather a dynamic and evolving framework. Organizations must continuously adjust their systems and processes to maintain resilience in response to new challenges and changing circumstances. This emphasizes the need for ongoing flexibility and proactive adjustments in resilience management.

Lastly, the cultural and behavioral foundations theme highlights that resilience is supported by organizational leadership, teamwork, and a proactive safety culture. This theme emerged from the category focused on organizational culture, where respondents recognized that resilience is not only about systems but also about the people who operate

within those systems. Leadership, collaboration, and a commitment to proactive safety behaviors are seen as critical components of a resilient organization, reinforcing the idea that resilience is as much about people and culture as it is about technical systems.

The quantitative and qualitative findings comprehensively show how practitioners perceive resilience-based approaches. While the quantitative data suggest that familiarity is generally moderate, the qualitative responses reveal that those with moderate familiarity often have a deeper understanding of resilience practices, such as anticipation, adaptability, and learning. This suggests that increased exposure and hands-on experience with resilience concepts could enhance their perceived usefulness among practitioners. The findings point to opportunities for training and capacity-building in resilience-based approaches, potentially improving the plant's overall safety and security.

3.4. Importance of Different Societal Values

In industrial settings, professionals frequently face challenging decisions that involve balancing the sometimes conflicting values of process safety and process security. This section examines how practitioners prioritize these values across five hypothetical risk scenarios, each presenting a trade-off between process safety and process security (Figure 6). The scenarios are briefly mentioned below, and full descriptions can be found in Appendix A.

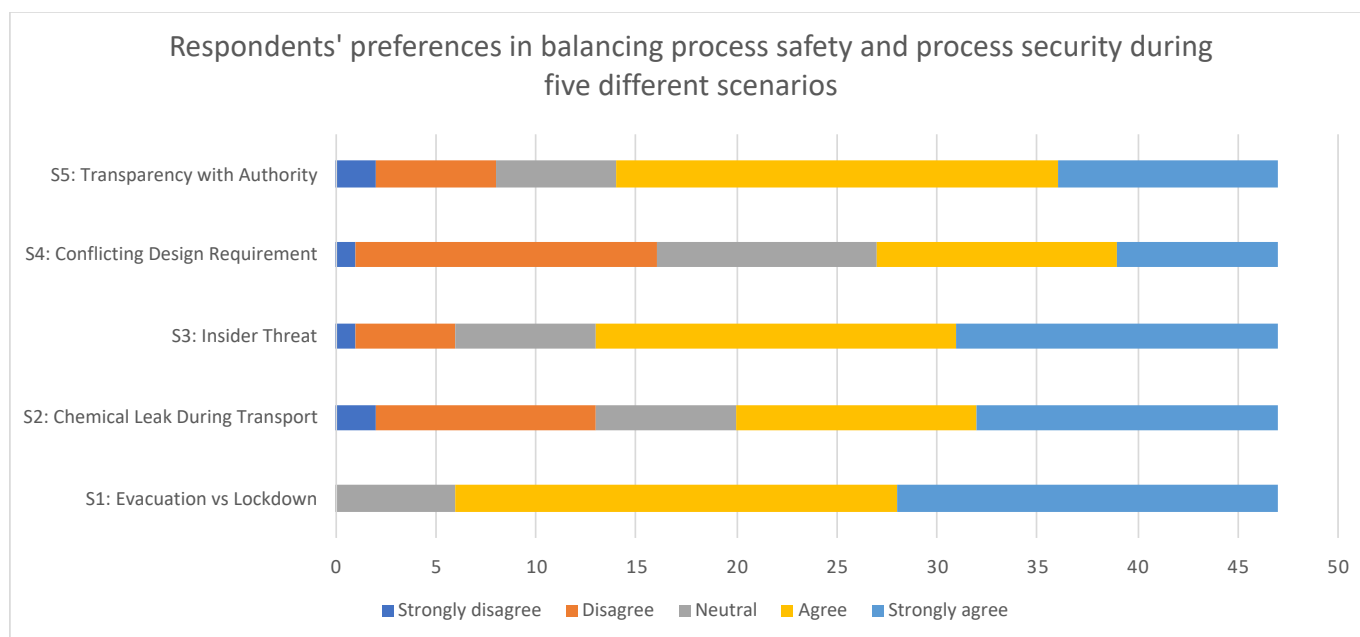


Figure 6. Respondents' preferences in balancing process safety and process security during five different scenarios.

In Scenario 1 (evacuation vs. lockdown), participants were asked to choose between executing an evacuation for process and personnel safety, even at the risk of exposing the site to security threats or opting for a lockdown to secure the site. An overwhelming majority (87%) agreed or strongly agreed that prioritizing evacuation for safety is the appropriate course of action. This reflects the strong preference for prioritizing life safety over site security in situations where personnel are at risk.

In Scenario 2 (chemical leak during transport), respondents considered whether to immediately inform the public about a chemical leak, prioritize safety, or secure the transport from potential threats before making any disclosures. A majority (57%) supported prioritizing public safety, but a notable proportion (28%) disagreed, showing concern for

securing hazardous materials first. This finding illustrates the complexity of balancing safety with security in scenarios involving hazardous substances.

In Scenario 3 (insider threat), respondents were asked to prioritize restricting access to chemicals to prevent potential misuse by an insider at the cost of disrupting regular operations. A strong majority (72%) agreed or strongly agreed with prioritizing security by restricting access. This demonstrates an apparent inclination toward process security measures when facing malicious threats, even if they compromise operational continuity.

In Scenario 4 (conflicting design requirements), respondents considered the importance of an open workspace design needed for safety audits versus security recommendations to limit access points. Responses were more divided, with 43% supporting the safety audit requirement, while 34% favored the security recommendation. This split indicates the difficulty practitioners face when operational safety and security requirements conflict, particularly in design-related decisions.

In Scenario 5 (transparency with regulatory bodies), participants were asked whether they would opt for full transparency with regulatory bodies, even if it exposed security vulnerabilities or limit the information to protect process security. A clear majority (70%) supported full transparency, reflecting the importance practitioners place on regulatory compliance and safety. However, 17% preferred limiting information to safeguard security, showing that security concerns remain significant, even in the face of regulatory transparency.

The analysis reveals a distinct pattern; in scenarios directly involving process and personnel safety, respondents tend to prioritize process safety over security concerns. This is evident in the strong support for evacuation (Scenario 1) and public communication during chemical leaks (Scenario 2). However, in scenarios emphasizing security threats, such as insider threats (Scenario 3) or design-related security vulnerabilities (Scenario 4), practitioners strongly prefer security measures, even at the expense of operational safety.

The responses to Scenario 5 reinforce this tendency. Although most respondents favored full transparency, suggesting that regulatory compliance and safety-driven transparency are critical, the notable portion of respondents who prioritized security indicates that security concerns are not entirely secondary. This demonstrates the nuanced balancing act practitioners must navigate when dealing with competing safety and security priorities.

These findings suggest that practitioners' values shift depending on the nature of the scenario. When personnel safety is at immediate risk, there is a clear preference for prioritizing safety, as seen in the evacuation and chemical leak scenarios. However, when security vulnerabilities or malicious actions are involved, practitioners lean toward security measures, such as restricting access or prioritizing security recommendations in design considerations. The divided responses in these scenarios highlight the complexity of these trade-offs and the need for careful decision-making in real-world situations.

The results from Scenario 5 suggest that while process security is important, regulatory compliance and safety-driven transparency take precedence. The tension between safety and security underscores the need for integrated frameworks that balance safety and security without compromising one for the other. Practitioners could benefit from tools and approaches that help them make informed decisions when process safety and process security come into conflict, ensuring that neither aspect is neglected in critical situations.

In addition to evaluating specific safety and security scenarios, respondents were asked to rank various societal values based on their importance in process safety and process security contexts [21]. The ranking, shown in Table 4, highlights key priorities in both domains and reveals some significant differences.

Table 4. Respondents' ranking of societal values in process safety and process security risk management (adapted from [19]).

Rank	Values in Process Safety	Rank	Values in Process Security
1	Risk reduction potential	1	Risk creation
2	Risk creation	2	Risk reduction potential
3	Jurisdictional authority	3	Cost
4	Effects on the environment	4	Timing
5	Timing	5	Jurisdictional authority
6	Leverage and compatibility	6	Leverage and compatibility
7	Cost	7	Effects on the environment
8	Administrative efficiency	8	Equity
9	Equity	9	Administrative efficiency
10	Fairness	10	Fairness

The two highest-ranked values across both process safety and process security were risk reduction potential and risk creation, but their order differs between the two domains. In process safety, risk reduction potential emerged as the top priority, indicating that practitioners prioritize actions that can prevent incidents and reduce losses. This reflects the core objective of process safety, which is minimizing harm and preventing accidents. Conversely, in process security, risk creation was ranked as the most important value, emphasizing that practitioners are more concerned with preventing the introduction of new risks or vulnerabilities, especially those related to malicious actions, such as theft or sabotage. This difference highlights the distinction between unintentional risks in safety and intentional risks in security. The focus on minimizing new risks in security suggests that the primary goal is not just to reduce existing risks but also to prevent any additional threats from emerging.

Jurisdictional authority ranked third in process safety but dropped to fifth in process security, suggesting that regulatory support and compliance are seen as slightly more critical in safety contexts. This could be due to the direct oversight that safety regulations often have on industrial operations, where ensuring compliance with safety standards is a top priority. In security, while still important, jurisdictional authority takes a backseat to other factors, such as cost and timing, reflecting the need for more immediate tactical responses to security threats.

Similarly, effects on the environment ranked fourth in process safety but seventh in process security, suggesting that practitioners see environmental impacts as more closely tied to safety incidents, where accidents like spills or fires can have immediate and direct effects on the environment. In process security, environmental concerns are less prominent, possibly due to the more focused goal of protecting assets and preventing malicious actions.

Cost was ranked higher in process security (third) than in process safety (seventh), reflecting the larger role that economic considerations play in security decisions. In the context of security, managing risks often involves strategic investments in protective measures, making cost a significant factor in decision-making. In contrast, in process safety, other values such as risk reduction potential and jurisdictional authority are seen as more pressing concerns, pushing cost lower on the list of priorities.

Timing, ranked fifth in process safety and fourth in process security, was consistently valued in both domains. This indicates that how quickly risk mitigation measures can be implemented is critical across both safety and security contexts. However, the slightly higher ranking in security suggests that there is a greater emphasis on responding swiftly to security threats, where delays and inaction could lead to serious consequences.

Values such as equity, fairness, and administrative efficiency were ranked lower in both process safety and process security. Fairness ranked last in both domains, indicating that concerns about the fair distribution of costs or responsibilities are often secondary to more immediate considerations such as risk reduction or cost-effectiveness.

Administrative efficiency was also ranked relatively low, eighth in process safety and ninth in process security. This suggests that while the ease of implementing risk management measures is considered, it is not a primary driver of decision-making in either domain. Practitioners appear more focused on achieving effective risk reduction than on whether the process is easy to administer.

In summary, the ranking shown in Table 4 highlights key priorities in both domains and reveals some important differences. These differences highlight the need for integrated risk management frameworks that can accommodate these varying priorities. Practitioners must be able to balance economic, environmental, and regulatory concerns while addressing both intentional risks in security and unintentional risks in safety. In conclusion, while many values are shared between process safety and process security, the differences in prioritization suggest that a holistic approach is needed to manage risks in both domains effectively.

3.5. Barriers and Enablers for Integration

In the survey, practitioners were asked to rank the main barriers to integrating process safety and process security risk management [17]. Lack of knowledge and awareness emerged as the most significant barrier (Figure 7). This highlights that many practitioners still lack a foundational understanding of how safety and security processes can be effectively integrated, representing a critical obstacle.

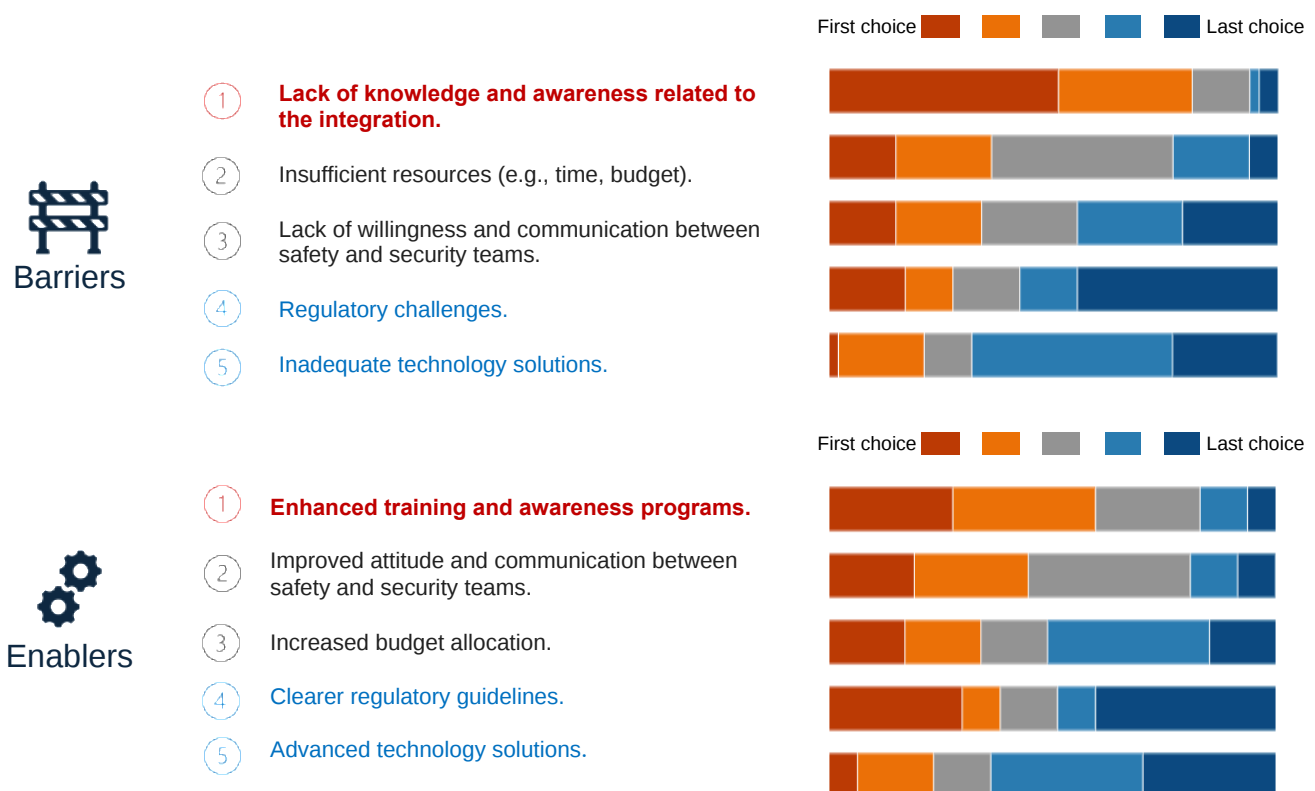


Figure 7. Ranking barriers and enablers for integrating process safety and security risk management (adapted from [19]).

The second-highest barrier was insufficient resources such as time, budget, and personnel. This may indicate that organizations struggle with resource constraints, which limits their ability to implement comprehensive integration strategies. For instance, budgetary limitations may prevent cross-disciplinary training, while time pressures may lead to short-term measures over integrated, long-term solutions. Lack of willingness and communication between safety and security teams emerged as the third major barrier.

Respondents cited in an open-ended response that poor communication and organizational silos are key challenges that prevent safety and security professionals from collaborating effectively. Regulatory challenges and inadequate technology solutions were ranked lower but remained relevant. Unclear or conflicting regulatory requirements and the need for better technological tools were noted by respondents, who emphasized the importance of aligning regulatory frameworks to support integration.

On the enabler side, enhanced training and awareness programs were identified as the top factor promoting successful integration. A respondent from the Netherlands stressed the need for *“knowledge on how to implement integration”*, highlighting the importance of targeted training. Improved communication and collaboration were the second most critical enabler, reflecting the need for coordinated efforts between safety and security teams. Increased budget allocation was the third-ranked enabler, which respondents saw as vital for supporting training, technology upgrades, and dedicated personnel. Lower-ranked enablers included clearer regulatory guidelines and advanced technology solutions, which respondents acknowledged could assist integration but were not seen as immediate priorities.

The qualitative analysis revealed key themes that further illuminate the complexity of integrating process safety and security (Figure 8). The intertwined nature of barriers was a prominent theme, where respondents identified a mix of organizational, technical, and regulatory challenges. For instance, a respondent from Malaysia noted the *“lack of communication and commitment”* between departments, while a respondent from the Netherlands highlighted inadequate regulatory enforcement as a barrier.

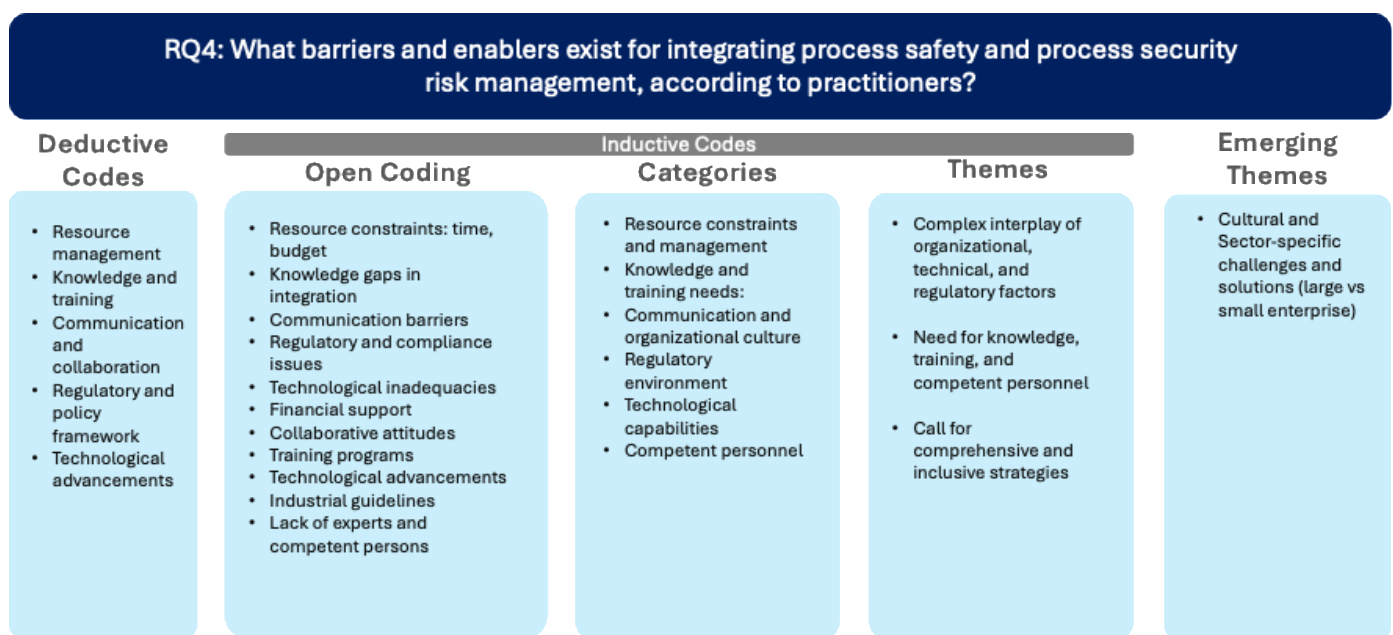


Figure 8. Thematic analysis matrix of barriers and enablers for integrating process safety and process security risk management.

Another key theme was the need for training and the development of competent personnel. Respondents pointed to knowledge gaps, with a respondent from Malaysia’s authority sector emphasizing the importance of *“management support”* in providing resources for training. Other respondents from the Netherlands emphasized the need for *“knowledge on how to implement integration”* and the development of *“common tools and language”* to address these gaps. Since the integration of process safety and security is relatively new, the lack of professionals trained in both domains creates a significant barrier.

Respondents also called for comprehensive strategies involving multiple stakeholders. A respondent from Malaysia emphasized the importance of regulatory support, stating the need to “*enhance regulation and enforcement*”. Ensuring top-down support and cross-departmental communication was viewed as essential for successful integration.

An emerging theme in the responses was the influence of cultural and sector-specific factors on the integration of process safety and security. Respondents from different regions and sectors highlighted distinct challenges. For instance, one participant remarked, “*they are two different worlds in our organization*”, pointing to the organizational silos between safety and security teams. Similarly, a respondent from Malaysia noted the “*lack of security risk awareness*”, suggesting that cultural attitudes toward security may lag behind those for safety, further complicating integration efforts.

This theme also underscores the importance of tailoring integration strategies to fit the specific context of each organization, including its size, resources, and operational complexity. Smaller enterprises commonly face resource constraints, with one respondent identifying “*budget and skilled personnel*” as key barriers. These organizations may benefit from solutions that focus on securing financial support and affordable technological tools. In contrast, larger organizations often struggle with communication inefficiencies and internal misalignment, requiring strategies to enhance interdepartmental communication and ensure unified safety and security policies.

In essence, lack of knowledge, resources, and communication were the primary barriers identified, while training, collaboration, and increased budget allocation were the key enablers. Integration strategies must be tailored to the specific organizational context, with smaller firms needing resource support and larger firms focusing on communication and policy alignment. Holistic strategies, including enhanced training, communication, and financial investment, are essential for effective integration across the process safety and security domains.

3.6. Proposed Strategies for Integrating Process Safety and Process Security

Respondents were asked to rate six proposed strategies for integrating process safety and security risk management [8,17]. These strategies included developing joint policies, conducting integrated risk assessments, and fostering clear communication channels. The quantitative data (Figure 9) provided insights into the perceived effectiveness of these strategies, with notable differences in ratings between respondents from Malaysia and the Netherlands.

Across all six strategies, respondents generally rated the approaches as either “Effective” or “Very Effective”. Conducting integrated risk assessments was the highest-rated strategy, with an average effectiveness score of 3.51 (3.61 in Malaysia and 3.18 in the Netherlands), emphasizing the importance of aligning risk assessment methodologies across both domains. Unified incident response and crisis management followed closely, with an overall score of 3.44, highlighting the need for coordinated responses to ensure swift resolution during both safety and security incidents.

Developing joint safety and security policies was rated 3.40 overall (3.47 in Malaysia and 3.18 in the Netherlands), underscoring the importance of having a structured framework for integration. Similarly, establishing clear communication channels between teams scored 3.40, with Malaysia rating it 3.53 compared to 3.00 in the Netherlands. Effective communication is critical for breaking down organizational silos.

However, strategies like cross-training safety and security personnel (3.21 overall) and utilizing integrated technology solutions (3.42 overall) received lower ratings, especially from Dutch respondents. These differences suggest regional or organizational variations

in the perceived feasibility of such measures, with Malaysian respondents being more favorable toward the use of technology and cross-training.

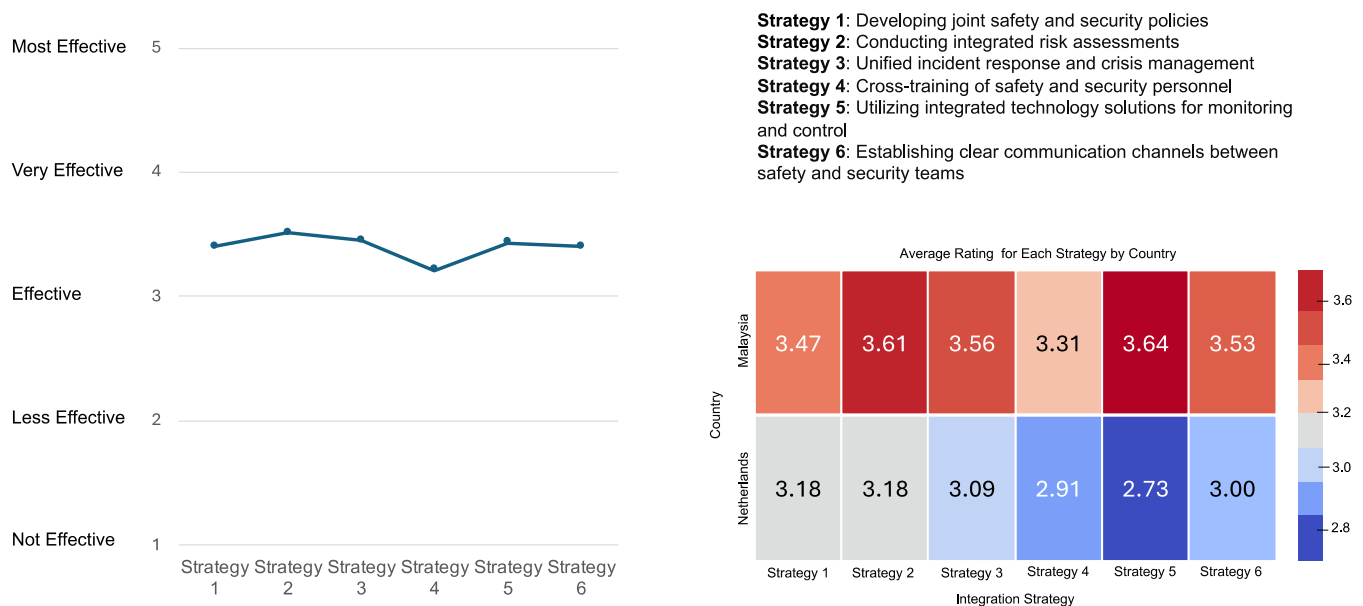


Figure 9. Respondents' rating on the effectiveness across six integration strategies.

A noticeable trend emerged when comparing responses from Malaysia and the Netherlands. Malaysian respondents consistently rated the proposed strategies higher than their Dutch counterparts. This may reflect cultural or organizational differences in how integration is approached in the two countries, with Malaysian practitioners potentially placing greater support on structured and proactive strategies.

A thematic analysis of open-ended responses revealed deeper insights into these strategies (Figure 10). Resilience-oriented risk management emerged as a key theme, with respondents emphasizing the need for proactive, adaptive strategies that balance safety and security. While not always explicitly rated as a standalone strategy, several respondents indirectly supported resilience principles through their emphasis on holistic risk and crisis management. One respondent suggested the creation of “*specific expert teams*” to focus on integrated risk assessments, while another stressed the importance of having clear guidelines for managing safety and security during crises. This highlights the importance of having a well-defined crisis management plan that integrates both safety and security considerations and supports resilience by ensuring that core functions are maintained even in the face of disruption.

Respondents also highlighted the need for integrated governance frameworks. Several called for “*merging regulations or guidelines*” to support alignment between safety and security. The role of top management was frequently mentioned, with one respondent noting that “*top management or the executor for safety and security should be the same person*”, stressing the need for unified leadership.

Training and awareness programs were consistently identified as critical enablers. Respondents advocated for “*awareness programs and training*” to equip practitioners with cross-disciplinary skills, bridging the knowledge gap between safety and security practices. Operational excellence, driven by strategic “*planning and budgeting*”, was also seen as crucial for successful integration.

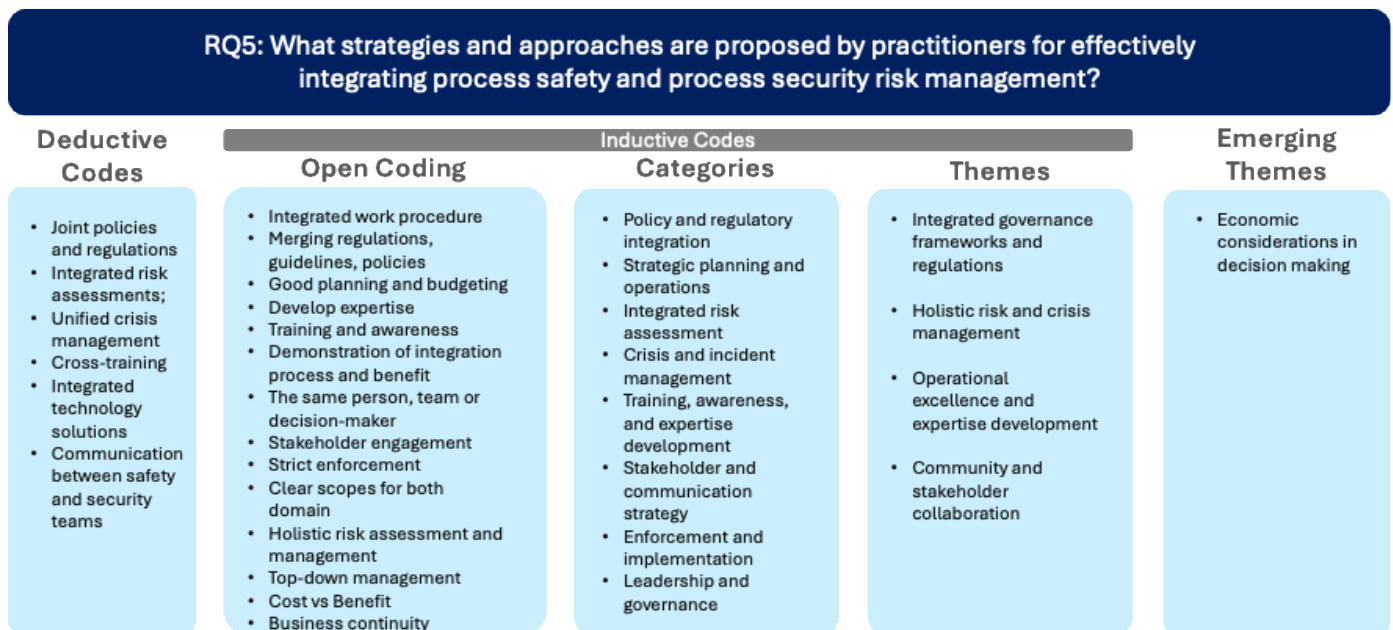


Figure 10. Thematic analysis matrix of strategies and approaches for integrating process safety and process security risk management.

Collaboration between stakeholders was another recurring theme. Respondents called for stronger communication between safety and security teams and with external stakeholders, such as regulators. One respondent suggested “*forums and feedback between all related parties*” to foster collaboration.

Finally, economic considerations played a key role in shaping integration strategies. Several respondents noted that financial investment is necessary for successful integration, with one respondent stating that “*business is willing to invest for such integration*”, indicating that organizations are likely to prioritize integration if it offers clear value.

In summary, both the quantitative and qualitative findings suggest the need for a comprehensive, resilience-oriented approach to integrating process safety and security. Key strategies include policy alignment, risk assessment, stakeholder collaboration, and tailored training programs supported by strong leadership and governance. By embedding resilience principles into these efforts, organizations can enhance their capacity to respond to and recover from both process safety and security threats, ultimately improving overall risk management.

4. Discussions

4.1. Interpretation of Findings

4.1.1. Integrating Process Safety and Security Risk Management

The survey findings emphasize the critical benefits and challenges of integrating process safety and security risk management. A total of 72% of respondents agreed that the integrated management of these two domains is beneficial. Qualitative analysis revealed that respondents recognized the intertwined nature of safety and security risks, advocating for a comprehensive and proactive approach.

One respondent (Malaysian authority personnel) noted that “In most cases, safety and security risks share the same hazard and effect. The differences would be in terms of intention (intentional vs. unintentional)”. This perspective aligns with the growing body of the literature that emphasizes the convergence of safety and security in high-risk industries, where integrating both domains is key to improving risk management outcomes [8,29,30]. Studies have shown that integrated frameworks reduce redundancies, enhance efficiency,

and improve overall risk management outcomes [16,17,31,32]. However, achieving integration remains challenging due to organizational silos, and differing priorities between safety and security teams remain significant barriers to attaining integration [19,29,33].

The findings also suggest that integration is a foundational element of resilience in chemical process industries, as it ensures comprehensive coverage of both unintentional and intentional risks [22,23,34]. Practical approaches to integration, as evidenced by the survey results (Figure 9), may include joint risk assessments and shared training programs for safety and security personnel. These strategies could enhance communication and collaboration, ultimately fostering more cohesive and resilient operations. For example, joint training sessions and drills could focus on scenarios incorporating both process safety and process security, encouraging cross-disciplinary understanding and teamwork.

4.1.2. Awareness and Usefulness of Resilience-Based Approaches

The survey revealed varying levels of familiarity with resilience-based approaches, with 76% of respondents indicating familiarity (slightly to very familiar) and 58% finding these approaches useful (and very useful) for managing process safety and process security risks. Practitioners with greater familiarity tended to perceive resilience-based approaches as highly beneficial, citing anticipation, adaptability, proactive risk identification, emergency response, and continuous improvement as key strengths. These findings align with the principles advocated by Pasman et al. (2020) [24] and Hollnagel (2016) [35], who emphasize that resilience engineering provides a dynamic and adaptive framework to address both intentional and unintentional risks.

One respondent illustrated this by stating “*Proactive learning from successful task or event*”. This statement reflects a core principle of resilience engineering, which is learning from both successes and failures to improve system robustness and adaptability [36–38]. As the literature highlights, such proactive learning is essential for enhancing process and organizational resilience in the face of disruptions [39,40].

However, the survey also highlighted variations in familiarity levels, which may reflect differences in organizational focus, roles, or geographic contexts. These variations underscore the need for education and training initiatives to increase awareness and understanding of resilience principles across the chemical process industry. As noted by Patriarca et al. (2018) [41], targeted training can enhance stakeholders’ capacity to anticipate and adapt to emerging risks, particularly in complex and dynamic environments. Similarly, Woods (2015) [42] emphasizes that scenario-based training is effective in fostering a shared understanding of adaptability and proactive risk management among multidisciplinary teams. The findings suggest practical strategies for leveraging resilience-based approaches, such as incorporating resilience principles into existing risk management frameworks or using scenario-based training to highlight adaptability and proactive risk identification. Addressing barriers, such as lack of familiarity or organizational inertia, will be critical to realizing the full potential of resilience engineering in practice [23,43].

4.1.3. Importance of Societal Values in Risk Management

Both the quantitative and qualitative data highlight the importance of aligning societal and organizational values—such as risk reduction, regulatory compliance, and operational efficiency—in supporting integrated risk management. This echoes findings in the risk management literature, where value alignment is seen as critical for creating a cohesive decision-making environment in a dynamic socio-technical system [21,44]. Among respondents, one of the most consistently prioritized values was “Risk reduction potential”, which ranked highly in both process safety and process security domains, demonstrating that shared values can minimize conflicts between safety and security objectives [32,45].

Focusing on shared values helps organizations create environments where process safety and process security objectives are mutually reinforcing rather than competitive [17]. This alignment facilitates the development of integrated risk management frameworks that prioritize safety, security, resilience, and business continuity [8,46].

However, aligning values in practice can be complex, mainly when trade-offs are necessary between competing objectives. For instance, regulatory compliance may sometimes emphasize security measures that inadvertently increase operational risks. Organizations can address these challenges through structured workshops and stakeholder consultations, prioritizing shared goals and mutual understanding [47,48]. Incorporating societal values into organizational policies and decision-making frameworks can further strengthen alignment, as suggested by De Bruijn and Herder (2009) [49]. These strategies enable organizations to create integrated risk management systems adaptable to evolving societal expectations and operational demands.

4.1.4. Barriers and Enablers for Effective Integration

The survey identified several barriers to the effective integration of process safety and security risk management, mirroring findings from previous studies on integration practices [17]. The most highly ranked barriers included a lack of knowledge and awareness, insufficient resources, and communication challenges between safety and security teams. For example, an academician from Malaysia noted *“Creating awareness at all levels on the significance for integrating process safety and process security risk management”*. These findings emphasize the need for enhanced training programs to build cross-disciplinary awareness and expertise, increased budget allocations to support integration efforts, and improved communication channels to foster collaboration.

In contrast, respondents also highlighted key enablers that could significantly support integration efforts. Management support was cited as a critical factor, with one respondent emphasizing that *“Management support is critical for driving integration and ensuring resources are allocated effectively”*. Regulatory alignment and the use of standardized tools and practices for risk assessment and mitigation were also frequently identified as enablers. These findings align with Schneller et al. (2023) [50], who identified leadership, regulatory frameworks, and collaborative tools as key facilitators in converged risk management strategies. Similarly, Gould and Bieder (2020) [29] emphasize the importance of fostering a cohesive culture to overcome organizational silos and promote integration.

The barriers and enablers identified in this study provide a clear roadmap for organizations seeking to integrate process safety and security risk management. For example, organizations could implement leadership training programs to equip managers with the skills to champion integration efforts. Similarly, adopting standardized risk assessment tools, as suggested by respondents, can help streamline processes and reduce silos between teams. These strategies underscore the importance of fostering a culture of collaboration and resilience to effectively overcome barriers and leverage enablers.

4.1.5. Effective Strategies for Integration

The study identified various strategies for effectively integrating process safety and security risk management, encompassing organizational and technical considerations. Developing joint safety and security policies, conducting integrated risk assessments, cross-training personnel, and utilizing integrated technology solutions were all identified as essential approaches. For instance, the suggestion to *“merge regulation or guideline”* reflects the need for coherent and unified regulatory frameworks that can support the dual objectives of safety and security.

Additionally, the emphasis on cross-training personnel points to the importance of equipping professionals with the skills and knowledge necessary to simultaneously manage both process safety and process security risks. Research highlights that training programs designed to build interdisciplinary skills can improve communication and foster mutual understanding across different domains [17,19]. Such training ensures that safety and security teams can collaborate effectively, leveraging shared knowledge to address overlapping risks [51,52].

To ensure the success of these strategies, organizations must implement robust performance indicators to monitor progress and evaluate the effectiveness of integration efforts [53–55]. Reniers et al. (2011) [56] suggest that performance indicators should encompass management, process, and result dimensions to provide a holistic view of risk management practices. For instance, metrics such as leadership commitment, the frequency of integrated risk assessments, and reductions in incident response times can offer actionable insights into areas requiring improvement. These indicators guide continuous improvement efforts and provide measurable evidence of integration success.

However, implementing these strategies requires addressing potential barriers, such as resource constraints, organizational inertia, and the need for cultural change [18,43,56]. For example, while joint policies and integrated tools can improve alignment, their adoption often requires significant investment and management buy-in. Practical approaches to overcome these challenges include establishing leadership roles dedicated to integration, securing funding through cost–benefit analyses, and promoting pilot programs to demonstrate the effectiveness of integrated strategies [56].

Overall, these strategies not only enhance operational efficiency but also strengthen process safety and process security. Organizations can create a more cohesive and adaptive risk management framework by adopting a systemic approach and fostering a system capable of addressing diverse threats and challenges.

4.2. *Synthesis of the Grand Themes*

The qualitative analysis of the survey responses offered a comprehensive view of the complexities and practical considerations involved in integrating process safety and security risk management. Several key themes emerged from the data, reflecting the interconnectedness of safety and security risks and providing insights into how practitioners perceive the integration process. The analysis of responses to the five research questions identified five overarching themes as critical to the successful integration of process safety and security risk management.

4.2.1. Theme 1: Proactive and Systemic Approach to Risk Management

A proactive and systemic approach to risk management emerged as a central theme across the responses. This theme aligns with the literature on integrated risk management, which highlights the necessity of addressing interdependent risks in a unified framework [11,56,57]. Respondents emphasized the interconnected nature of safety and security risks and advocated for a structured and proactive strategy to manage these risks. This approach involves mutual risk identification, resource optimization, and the strategic integration of expertise. Many respondents highlighted the benefits of adopting a more holistic view, where process safety and security are not treated as isolated silos but as interdependent components of a comprehensive risk management framework. Leveson et al. (2014) [51] argued that a systemic approach to risk management can streamline operations and create a more resilient process system.

4.2.2. Theme 2: Resilience-Oriented Systems and Processes

Resilience was another dominant theme, with respondents underlining the importance of adaptability, emergency response, and business continuity. Resilience-based approaches focus on proactive measures, including anticipation and rapid recovery from disruptions, consistent with resilience engineering frameworks [37,58,59]. Resilience enables organizations to absorb and recover from both unintentional and malicious threats, particularly in a complex engineered system such as the CPI [23,57]. One respondent noted a resilience-oriented approach as *“Proactive learning from successful task or event”*, reflecting key principles from the resilience literature. The focus on anticipation and continuous improvement aligns with the *“adaptive capacity”* concept in resilience theory, which is critical for managing risks in dynamic environments [24].

4.2.3. Theme 3: Strategic Alignment of Societal Values

The strategic alignment of values was also identified as a crucial factor for successful integration. Respondents stressed the need to align societal values, such as risk reduction, regulatory compliance, and operational efficiency, to support integrated risk management. This alignment is essential for minimizing conflicts and enhancing decision-making processes [45,60]. By aligning values across process safety and process security domains, organizations can create a more cohesive and effective risk management strategy [17].

4.2.4. Theme 4: Leadership, Governance, and Collaboration

Effective leadership, governance, and collaboration emerged as one of the key enablers for integrating process safety and security risk management. Respondents identified strong leadership and governance structures that support cross-functional collaboration as vital for fostering system resilience. The importance of clear communication channels and collaborative efforts between process safety and security teams was frequently mentioned. As noted by one respondent, *“Top management or executer for safety and security operations and measures are same person”*, which could be an effective strategy. Similarly to the literature, this study also suggested that organizational leadership should actively promote and support integration efforts to ensure their success [56,61].

4.2.5. Theme 5: Continuous Improvement and Adaptation

The theme of continuous improvement and adaptation was prominent in the qualitative responses, aligning with the literature on adaptive risk management and organizational learning [21,32,44]. Respondents highlighted the need for ongoing learning and adaptation, leveraging new technologies and data analytics to enhance system resilience. Proactive learning, system reviews, and integrating behavioral studies into risk management practices were critical for maintaining and improving resilience. Respondents advocated for a dynamic approach to risk management that evolves with changing conditions and emerging threats.

Together, these five themes provide a conceptual yet robust foundation for developing practical strategies to enhance risk management practices within the chemical process industry. The emphasis on resilience, strategic alignment of values, and continuous improvement underscores the importance of building adaptive, proactive, and unified systems that effectively manage process safety and process security risks. By integrating leadership support, collaboration, and systemic approaches into their organizational frameworks, companies can strengthen their operational resilience and create a safer and more secure industrial environment.

4.3. Recommendations

This study offers practical recommendations for integrating process safety and security risk management in the chemical process industry, informed by survey findings and supported by the existing literature. These recommendations are designed to address interconnected risks, enhance operational resilience, and foster a unified approach to risk management.

Firstly, organizations should adopt a comprehensive and proactive approach to managing process safety and security risks. The survey findings revealed that 72% of respondents recognized the benefits of integration, emphasizing the need for a unified framework. Regular joint risk assessments and scenario planning exercises are essential for identifying overlapping vulnerabilities and preparing for potential disruptions. For example, integrating process hazard analysis with security vulnerability assessments can streamline processes and improve resource allocation. Such approaches align with systemic risk management strategies advocated by Leveson et al. (2014) [51], which focus on addressing interdependencies to enhance resilience.

Secondly, organizations should establish performance indicators to monitor and evaluate the effectiveness of resilience-oriented process safety and security risk management frameworks [62]. Respondents highlighted the importance of clear metrics to ensure continuous progress in integrating safety and security practices. Building on Reniers et al. (2011) [56], these indicators could cover management, process, and result metrics, providing a comprehensive view of how well the integration is functioning. Management indicators might focus on leadership commitment, resource allocation, and cross-functional collaboration. Process indicators could assess the frequency and quality of integrated risk assessments, cross-training initiatives, and the adoption of advanced technologies. Result indicators might measure incident response times, reductions in risk exposure, and overall system resilience. By regularly tracking these performance indicators, organizations can identify areas for improvement and ensure continuous progress in strengthening both safety and security efforts.

Additionally, aligning societal values like risk reduction, environmental stewardship, and operational efficiency is equally critical to achieving cohesive risk management strategies. Survey findings indicated that “risk reduction potential” was highly prioritized, highlighting its centrality in both safety and security domains. Organizations can achieve value alignment by developing policies that reflect shared values such as environmental stewardship, operational efficiency, and regulatory compliance. Structured workshops and stakeholder consultations can further facilitate dialog to align goals and enhance decision-making. De Bruijn and Herder (2009) [49] suggest that aligning values fosters cohesive decision-making within complex socio-technical systems.

Furthermore, ongoing investment in continuous improvement and advanced technology, such as real-time monitoring and data analytics, is critical for enhancing risk management. Emerging technologies such as digital twins and machine learning (ML) offer additional opportunities for improving risk management. Digital twins can simulate process scenarios, enabling a proactive identification of vulnerabilities and testing of integrated safety–security strategies [63,64]. ML algorithms can enhance predictive capabilities, detecting patterns in operational data to anticipate risks and optimize mitigation efforts [65]. Leveraging these tools enables data-driven assessments and strengthens system resilience.

Finally, leadership plays a pivotal role in promoting integration efforts. Senior management should allocate necessary resources, foster a culture of collaboration, and establish dedicated roles to oversee integration initiatives [56]. Leaders should also encourage collaboration between safety and security teams through joint training programs and clear communication channels [19]. Pilot programs and a phased implementation of strate-

gies can demonstrate their effectiveness, build organizational confidence, and ensure sustained progress.

These recommendations aim to create an adaptive and unified framework that enhances operational efficiency, strengthens resilience, and ensures the safe and secure operation of chemical process industries.

5. Conclusions

Integrating process safety and security risk management is essential for enhancing resilience in the chemical process industry, particularly in increasingly complex and interconnected operational environments. This study highlights the intertwined nature of safety and security risks, with 72% of respondents agreeing that integration is beneficial. Organizations can optimize resource utilization, improve risk mitigation, and enhance operational efficiency by addressing these interdependencies.

While this study employs a mixed-methods approach, the findings primarily aim to explore practitioner perspectives and generate qualitative insights into the integration of process safety and security rather than achieving broad generalizability. Based on a diverse sample of 47 practitioners, the findings reveal significant barriers to integration, including knowledge gaps, resource constraints, and communication challenges. Addressing these barriers requires targeted interventions such as enhanced training programs, management support, and regulatory alignment. Critical enablers identified in this study, such as leadership commitment, cross-functional collaboration, and the adoption of advanced technologies, are pivotal for fostering organizational change and resilience.

To support integration, this study proposes actionable strategies such as establishing robust performance indicators to monitor and evaluate progress. Metrics like leadership engagement, incident response times, and system resilience provide measurable insights into integration effectiveness. Advanced technologies such as digital twins and machine learning offer further opportunities by enabling proactive risk management through scenario simulation and predictive analytics. These technologies can help organizations identify vulnerabilities, optimize mitigation strategies, and enhance overall resilience.

Though this study provides valuable insights, several limitations must be acknowledged. The sample size limits the generalizability of findings, and reliance on self-reported data introduces potential biases. Future research could address these limitations by expanding the scope to other high-risk sectors, such as healthcare, transportation, and energy and by employing longitudinal designs to assess the long-term effectiveness of integration efforts. Additionally, in-depth qualitative methods, such as interviews and case studies, could provide richer narratives and deeper insights into organizational dynamics and the practical applications of integration strategies.

The role of advanced technologies in supporting integration is another promising avenue for future research. Exploring the adoption and impact of real-time monitoring, data analytics, and AI-driven tools across industries could provide critical insights for developing more sophisticated integrated frameworks.

In conclusion, this study provides both theoretical and practical contributions to the integration of process safety and security risk management. It lays the groundwork for developing a unified, resilience-oriented framework to address integration challenges and enhance risk management practices. By tackling identified barriers, implementing proposed strategies, and exploring the outlined research directions, organizations can advance toward a cohesive and adaptive approach to risk management. These findings serve as a call to action for practitioners, policymakers, and researchers to collaboratively foster resilience and create safer, more secure industrial environments.

Author Contributions: Conceptualization, M.S.A.R., G.R. and M.Y.; methodology, M.S.A.R., G.R. and P.S.; software, M.S.A.R.; validation, M.S.A.R. and M.Y.; formal analysis, M.S.A.R.; data curation, M.S.A.R.; writing—original draft preparation, M.S.A.R.; writing—review and editing, G.R., M.Y. and P.S.; visualization, M.S.A.R.; supervision, G.R. and M.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The survey questionnaire and anonymized dataset used in this study are available through the publicly accessible research repository 4TU.ResearchData at <https://data.4tu.nl/datasets/4522882f-0d76-46ad-b63f-5344964e1fb8>, accessed on 2 January 2025.

Acknowledgments: This work was supported by the Public Service Department of Malaysia through the Federal Training Prize 2022 (reference number JPA(1)830227015745). We thank all the professionals who participated in the survey, as well as the Department of Occupational Safety and Health Malaysia, particularly Fairuz Anwar and Kasman Nasir, for their support in survey distribution. This article is a revised and expanded version of a conference paper entitled “Bridging Boundaries: Crafting a Resilient, Integrated Risk Management Model for Process Safety and Process Security”, which was presented at the International Conference on Safety & Environment In Process & Power Industry (CISAP 11), held from 15 to 18 September 2024 in Naples, Italy (Chemical Engineering Transactions, DOI: 10.3303/CET24111023).

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

Balancing societal values within process safety and process security.

In the management of industrial processes, professionals often encounter situations where the societal values related to process safety and process security may not fully align. These scenarios can present challenging decisions where prioritizing one value may lead to compromises in the other. Below, we present a series of hypothetical scenarios that illustrate potential conflicts between process safety and process security. Your responses to these scenarios will help us understand how practitioners like yourself might prioritize in these complex situations.

Please consider each scenario carefully and indicate your level of agreement with the proposed course of action using the scale provided, where 1 represents “Strongly Disagree” and 5 represents “Strongly Agree”.

Scenario 1: Evacuation vs. Lockdown

In an emergency where a quick evacuation could expose the site to security risks, executing the evacuation to prioritize personnel and process safety is more important than opting for a lockdown to protect the site from potential threats.

Scenario 2: Unexpected Chemical Leak During Transport

In the event of an unexpected chemical leak during transport, informing the public immediately to ensure safety is more important than securing the transport from potential threats before making any disclosures.

Scenario 3: Insider Threat

If there is suspicion of an insider threat intending to misuse chemicals, restricting all staff access to chemicals to prevent any malicious harm is more important than continuing regular operations.

Scenario 4: Conflicting Design Requirements

When an open workspace design required for safety audits conflicts with security advice to limit access points, prioritizing the safety audit requirements is more important than following the security recommendations to limit access.

Scenario 5: Transparency with Regulatory Bodies

If providing complete transparency to a regulatory body about safety processes inadvertently reveals security vulnerabilities, opting for full disclosure is more important than limiting the information provided to protect against security risks.

References

- Center for Chemical Process Safety. Guidelines for Risk Based Process Safety. In *American Institute of Chemical Engineers*; Wiley: Hoboken, NJ, USA, 2007. [CrossRef]
- Occupational Safety and Health Administrations (OSHA). *Process Safety Management of Highly Hazardous Chemicals Standard* (29 CFR 1910.119); OSHA: Washington, DC, USA, 1992. Available online: <https://www.osha.gov/process-safety-management> (accessed on 12 November 2024).
- European Union. Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the Control of Major-Accident Hazards Involving Dangerous Substances (Seveso III). 2012, pp. 1–37. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018> (accessed on 12 November 2024).
- Kannan, P.; Flechas, T.; Mendez, E.; Angarita, L.; Chaudhari, P.; Hong, Y.; Mannan, M.S. A web-based collection and analysis of process safety incidents. *J. Loss Prev. Process Ind.* **2016**, *44*, 171–192. [CrossRef]
- Jain, P.; Pasman, H.J.; Waldram, S.P.; Rogers, W.J.; Mannan, M.S. 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.* **2017**, *49*, 5–17. [CrossRef]
- Khan, F.; Rathnayaka, S.; Ahmed, S. Methods and models in process safety and risk management: Past, present and future. *Process Saf. Environ. Prot.* **2015**, *98*, 116–147. [CrossRef]
- Leveson, N.G. Applying systems thinking to analyze and learn from events. *Saf. Sci.* **2011**, *49*, 55–64. [CrossRef]
- Rahim, M.S.A.; Reniers, G.; Yang, M.; Bajpai, S. Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review. *J. Loss Prev. Process Ind.* **2024**, *88*, 105274. [CrossRef]
- DHS; DOL; EPA; OSHA. Executive Order 13650 Actions to Improve Chemical Safety and Security—A Shared Commitment. 2014. Available online: https://www.osha.gov/sites/default/files/final_chemical_eo_status_report.pdf (accessed on 12 November 2024).
- Pasman, H.J.; Knegtering, B.; Rogers, W.J. A holistic approach to control process safety risks: Possible ways forward. *Reliab. Eng. Syst. Saf.* **2013**, *117*, 21–29. [CrossRef]
- Ta, G.C.; Amir Sultan, M.M.; Lee, K.E.; Mokhtar, M.; Tan, L.L.; Omar, A.S.; Omar, M.N.; Sulkafle, N.H. A Proposed Integrated Framework for Chemical Safety and Chemical Security. *J. Chem. Educ.* **2020**, *97*, 1769–1774. [CrossRef]
- Moorel, D.A. The new risk paradigm for chemical process security and safety. *J. Hazard. Mater.* **2004**, *115*, 175–180. [CrossRef] [PubMed]
- Iaiani, M.; Moreno, V.C.; Reniers, G.; Tugnoli, A.; Cozzani, V. Analysis of events involving the intentional release of hazardous substances from industrial facilities. *Reliab. Eng. Syst. Saf.* **2021**, *212*, 107593. [CrossRef]
- Varadharajan, S.; Bajpai, S. Chronicles of security risk assessment in process industries: Past, present and future perspectives. *J. Loss Prev. Process Ind.* **2023**, *84*, 105096. [CrossRef]
- Matteini, A.; Argenti, F.; Salzano, E.; Cozzani, V. A comparative analysis of security risk assessment methodologies for the chemical industry. *Reliab. Eng. Syst. Saf.* **2019**, *191*, 106083. [CrossRef]
- Amin, T.; Khan, F.; Halim, S.Z.; Pistikopoulos, S. A holistic framework for process safety and security analysis. *Comput. Chem. Eng.* **2022**, *165*, 107963. [CrossRef]
- Ylönen, M.; Argenti, F.; Salzano, E.; Cozzani, V. Integrated management of safety and security in Seveso sites—Sociotechnical perspectives. *Saf. Sci.* **2022**, *151*, 105741. [CrossRef]
- OPCW. *Indicative Guidelines for Chemical Safety and Security in Small and Medium-Sized Enterprises to Foster the Peaceful Uses of Chemistry*; OPCW: The Hague, The Netherlands, 2021.
- Rahim, M.S.A.; Reniers, G.; Yang, M. Bridging Boundaries: Crafting a Resilient, Integrated Risk Management Model for Process Safety and Process Security. In *Chemical Engineering Transactions*; Italian Association of Chemical Engineering—AIDIC: Bologna, Italy, 2024; pp. 133–138. [CrossRef]
- van de Poel, I. Design for value change. *Ethics Inf. Technol.* **2021**, *23*, 27–31. [CrossRef]
- Meyer, T.; Reniers, G.L.L. *Engineering Risk Management*, 3rd ed.; De Gruyter: Berlin, Germany, 2022.
- Aven, T. The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Anal.* **2019**, *39*, 1196–1203. [CrossRef] [PubMed]
- Yang, M.; Sun, H.; Geng, S. On the quantitative resilience assessment of complex engineered systems. *Process Saf. Environ. Prot.* **2023**, *174*, 941–950. [CrossRef]
- Pasman, H.; Kottawar, K.; Jain, P. Resilience of process plant: What, why, and how resilience can improve safety and sustainability. *Sustainability* **2020**, *12*, 6152. [CrossRef]

25. Yu, M.; Quddus, N.; Kravaris, C.; Mannan, M.S. Development of a FRAM-based framework to identify hazards in a complex system. *J. Loss Prev. Process Ind.* **2020**, *63*, 103994. [\[CrossRef\]](#)
26. Noor, M.Z.M. *Illustrasi Ringkas Analisa Tematik (AT) Menggunakan Perisian ATLAS*; UPM Press: Putra, Malaysia, 2021.
27. Zou, P.X.W.; Sunindijo, R.Y.; Dainty, A.R.J. A mixed methods research design for bridging the gap between research and practice in construction safety. *Saf. Sci.* **2014**, *70*, 316–326. [\[CrossRef\]](#)
28. Stantcheva, S. How to Run Surveys: A Guide to Creating Your Own Identifying Variation and Revealing the Invisible. *Annu. Rev. Econom.* **2023**, *15*, 205–234. [\[CrossRef\]](#)
29. Gould, K.P.; Bieder, C. Safety and Security: The Challenges of Bringing Them Together. In *SpringerBriefs in Applied Sciences and Technology*; Springer Science and Business Media Deutschland GmbH: Berlin/Heidelberg, Germany, 2020; pp. 1–8. [\[CrossRef\]](#)
30. El-Kady, A.H.; Halim, S.; El-Halwagi, M.M.; Khan, F. Analysis of Safety and Security Challenges and Opportunities Related to Cyber-physical Systems. *Process Saf. Environ. Prot.* **2023**, *173*, 384–413. [\[CrossRef\]](#)
31. Bischoff, H.-J.; Sinay, J.; Vargová, S. Integrated Risk Management in Industries from the Standpoint of Safety and Security. *Saf. Eng. Ser.* **2015**, *9*, 1–7. [\[CrossRef\]](#)
32. Kriaa, S.; Pietre-Cambacedes, L.; Bouissou, M.; Halgand, Y. A survey of approaches combining safety and security for industrial control systems. *Reliab. Eng. Syst. Saf.* **2015**, *139*, 156–178. [\[CrossRef\]](#)
33. Baybutt, P. Issues for security risk assessment in the process industries. *J. Loss Prev. Process Ind.* **2017**, *49*, 509–518. [\[CrossRef\]](#)
34. Jain, P.; Mentzer, R.; Mannan, M.S. Resilience metrics for improved process-risk decision making: Survey, analysis and application. *Saf. Sci.* **2018**, *108*, 13–28. [\[CrossRef\]](#)
35. Hollnagel, E. Resilience Engineering: A New Understanding of Safety. *J. Ergon. Soc. Korea* **2016**, *35*, 185–191. [\[CrossRef\]](#)
36. Hollnagel, E.; Woods, D.D.; Leveson, N. *Resilience Engineering: Concepts and Precepts*; Ashgate Publishing Ltd.: Farnham, UK, 2012. [\[CrossRef\]](#)
37. Jain, P.; Pasman, H.J.; Waldram, S.; Pistikopoulos, E.N.; Mannan, M.S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *J. Loss Prev. Process Ind.* **2018**, *53*, 61–73. [\[CrossRef\]](#)
38. Aven, T. How some types of risk assessments can support resilience analysis and management. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 536–543. [\[CrossRef\]](#)
39. Jain, P.; Rogers, W.J.; Pasman, H.J.; Mannan, M.S. A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer. *Process Saf. Environ. Prot.* **2018**, *118*, 115–124. [\[CrossRef\]](#)
40. Yarveisy, R.; Sun, H.; Yang, M.; Pasman, H. *Resilience Analysis of Digitalized Process Systems*; Elsevier: Amsterdam, The Netherlands, 2022; pp. 591–629. [\[CrossRef\]](#)
41. Patriarca, R.; Bergström, J.; Di Gravio, G.; Costantino, F. *Resilience Engineering: Current Status of the Research and Future Challenges*; Elsevier B.V.: Amsterdam, The Netherlands, 2018. [\[CrossRef\]](#)
42. Woods, D.D. Four concepts for resilience and the implications for the future of resilience engineering. *Reliab. Eng. Syst. Saf.* **2015**, *141*, 5–9. [\[CrossRef\]](#)
43. Jahangiri, M.; Zinat-Motlagh, K.; Ghaem, H.; Zinat-Motlagh, F.; Kamalinia, M.; Banaee, S. Safety culture maturity and resilience engineering in an oil drilling industry: A comparison study among government-owned and private companies. *Work* **2021**, *70*, 443–453. [\[CrossRef\]](#) [\[PubMed\]](#)
44. Rasmussen, J. Risk management in a dynamic society: A modelling problem. *Saf. Sci.* **1997**, *27*, 183–213. [\[CrossRef\]](#)
45. Reniers, G.; Landucci, G.; Khakzad, N. What safety models and principles can be adapted and used in security science? *J. Loss Prev. Process Ind.* **2020**, *64*, 104068. [\[CrossRef\]](#)
46. Jain, P.; Pasman, H.J.; Mannan, M.S. Process system resilience: From risk management to business continuity and sustainability. *Int. J. Bus. Contin. Risk Manag.* **2020**, *10*, 47–66. [\[CrossRef\]](#)
47. Ktori, R.; Parada, M.P.; Rodriguez-Pascual, M.; van Loosdrecht, M.C.M.; Xevgenos, D. A value-sensitive approach for integrated seawater desalination and brine treatment. *Sustain. Prod. Consum.* **2024**, *52*, 363–377. [\[CrossRef\]](#)
48. Jayaraman, S.N.B.F.R.; Shariff, A.M.; Zaini, D. Stakeholder outreach on process safety for process industry using risk based approaches. *Process Saf. Prog.* **2020**, *39*, 12130. [\[CrossRef\]](#)
49. de Bruijn, H.; Herder, P.M. System and actor perspectives on sociotechnical systems. *IEEE Trans. Syst. Man Cybern. Part A Syst. Hum.* **2009**, *39*, 981–992. [\[CrossRef\]](#)
50. Schneller, L.; Porter, C.N.; Wakefield, A. Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators. *Secur. J.* **2023**, *36*, 333–349. [\[CrossRef\]](#)
51. Leveson, N.G.; Stephanopoulos, G. A System-Theoretic, Control-Inspired View and Approach to Process Safety. *AiChE J.* **2014**, *60*, 2–14. [\[CrossRef\]](#)
52. Fouzi, N.F.R.; Aziz, H.A.; Yaakub, N. *Systematic Review of Chemical Safety and Chemical Security Risk Management Approach*; Institution of Chemical Engineers: Rugby, UK, 2024. [\[CrossRef\]](#)
53. Jovanović, A.; Øien, K.; Choudhary, A. An indicator-based approach to assessing resilience of smart critical infrastructures. In *Urban Book Series*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 285–311. [\[CrossRef\]](#)

54. Khan, F.; Abunada, H.; John, D.; Benmosbah, T. Development of risk-based process safety indicators. *Process Saf. Prog.* **2010**, *29*, 133–143. [\[CrossRef\]](#)
55. Pasman, H.; Rogers, W. How can we use the information provided by process safety performance indicators? Possibilities and limitations. *J. Loss Prev. Process Ind.* **2014**, *30*, 197–206. [\[CrossRef\]](#)
56. Reniers, G.L.L.; Cremer, K.; Buytaert, J. Continuously and simultaneously optimizing an organization's safety and security culture and climate: The Improvement Diamond for Excellence Achievement and Leadership in Safety & Security (IDEAL S&S) model. *J. Clean. Prod.* **2011**, *19*, 1239–1249. [\[CrossRef\]](#)
57. Logan, T.M.L.; Aven, T.; Guikema, S.D.; Flage, R. Risk science offers an integrated approach to resilience. *Nat. Res.* **2022**, *5*, 741–748. [\[CrossRef\]](#)
58. Yarveisy, R.; Gao, C.; Khan, F. A simple yet robust resilience assessment metrics. *Reliab. Eng. Syst. Saf.* **2020**, *197*, 106810. [\[CrossRef\]](#)
59. Cheng, Y.; Elsayed, E.A.; Huang, Z. Systems resilience assessments: A review, framework and metrics. *Int. J. Prod. Res.* **2022**, *60*, 595–622. [\[CrossRef\]](#)
60. Amundrud, Ø.; Aven, T.; Flage, R. How the definition of security risk can be made compatible with safety definitions. *Proc. Inst. Mech. Eng. O J. Risk Reliab.* **2017**, *231*, 286–294. [\[CrossRef\]](#)
61. Reniers, G.L.L. *Multi-Plant Safety and Security Management in the Chemical and Process Industries*; Wiley: Hoboken, NJ, USA, 2010. [\[CrossRef\]](#)
62. Leveson, N. A systems approach to risk management through leading safety indicators. *Reliab. Eng. Syst. Saf.* **2015**, *136*, 17–34. [\[CrossRef\]](#)
63. Bevilacqua, M.; Bottani, E.; Ciarapica, F.E.; Costantino, F.; Di Donato, L.; Ferraro, A.; Mazzuto, G.; Monteriù, A.; Nardini, G.; Ortenzi, M.; et al. Digital Twin Reference Model Development to Prevent Operators' Risk in Process Plants. *Sustainability* **2020**, *12*, 1088. [\[CrossRef\]](#)
64. Alsuliman, A.; Ge, X.; Zeng, Z.; Butenko, S.; Khan, F.; El-Halwagi, M. Dynamic risk analysis of evolving scenarios in oil and gas separator. *Reliab. Eng. Syst. Saf.* **2024**, *243*, 109843. [\[CrossRef\]](#)
65. Raveendran, A.; Renjith, V.R.; Madhu, G. A comprehensive review on dynamic risk analysis methodologies. *J. Loss Prev. Process Ind.* **2022**, *76*, 104734. [\[CrossRef\]](#)

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.