Process Safety and Environmental Protection 215 (2026) 109182

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

A resilience-oriented framework for managing process safety and process security

Muhammad Shah Ab Rahim [a,b,*], Genserik Reniers [a,c,d], Ming Yang [a]

[a] Safety and Security Science Section, Faculty of Technology, Policy and Management, Delft University of Technology, Delft 2628 BX, the Netherlands
[b] Department of Occupational Safety and Health Malaysia, Ministry of Human Resources, Federal Government Administrative Centre, Putrajaya 62530, Malaysia
[c] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), Universiteit Antwerpen, Antwerp 2000, Belgium
[d] Centre for Economics and Corporate Sustainability (CEDON), KU Leuven, Brussels 1000, Belgium

ARTICLE INFO

Keywords:
Resilience engineering
Process safety
Process security
Integrated risk management
Performance indicators
Chemical process industry
Coupled safety-security risk

ABSTRACT

Process safety and process security share the common goal of protecting people, assets, and the environment, yet they remain largely fragmented in regulation and practice. This separation obscures the coupled nature of accidental and intentional risks in the chemical process industry and creates blind spots in how safety–security interactions are managed. To address this challenge, this study develops the Resilience-oriented Process Safety and Process Security (RoPSS) framework, which integrates both domains through four resilience capabilities (Anticipation, Absorption, Adaptation, and Ascension) embedded within a six-step management cycle. The framework introduces Ascension as an evolutionary capability that consolidates restoration, learning, continuous improvement, and prevention, extending resilience beyond recovery toward longer-term system strengthening. A structured catalogue of 50 performance indicators, organized by disruption type, resilience capability, and indicator category, provides measurable means to assess both operational and governance resilience. These indicators were defined and refined through focused expert elicitation, including an importance-availability assessment used as a formative step for indicator prioritization. An illustrative example in a chlor-alkali plant shows how RoPSS supports integrated disruption mapping, shared objective setting, and resilience-enhancing strategies. Overall, the framework offers an expert-informed conceptual basis for managing coupled safety–security risks and provides a foundation for future empirical evaluation, industrial application, and resilience benchmarking.

1. Introduction

The chemical process industry (CPI) operates under high-hazard operations due to the handling of flammable, toxic, and reactive substances combined with complex, energy-intensive, and increasingly digitalized operations (CCPS, 2007; Yuan et al., 2024). These socio-technical systems integrate physical processes, control technologies, and human decision-making in ways that can generate nonlinear and cascading consequences when disturbances occur (Yang et al., 2023). The potential for major accidents has long motivated the development of stringent regulatory and managerial systems to prevent, mitigate, and recover from such events (EU Directive 2012/18/EU, 2012; US 29 CFR § 1910.119, 1992). However, as automation, digitalization, and global interconnection accelerate, the traditional boundaries between safety and security have become increasingly blurred (Hansen and Antonsen, 2024; Ylönen et al., 2022).

Within the complexity of CPI, process safety and process security share the overarching goal of protecting people, the environment, and assets, yet they address different sources of risk (Ab Rahim et al., 2024; Yuan et al., 2025). Process safety focuses on unintentional events, such as equipment failure, human error, or loss of containment, whereas process security seeks to deter and manage intentional acts, including terrorism, sabotage, or cyber intrusion (Reniers et al., 2020). Despite these shared objectives, the two domains have evolved along separate regulatory regimes. Frameworks such as the EU Seveso III Directive and the US OSHA Process Safety Management standard address major accident hazards. In contrast, process security is governed indirectly through broader counterterrorism, chemical control, physical

* Corresponding author at: Safety and Security Science Section, Faculty of Technology, Policy and Management, Delft University of Technology, Delft 2628 BX, the Netherlands.
E-mail address: a.r.m.s.binabrahim@tudelft.nl (M.S.A. Rahim).

https://doi.org/10.1016/j.psep.2026.109182
Received 10 December 2025; Received in revised form 12 June 2026; Accepted 18 June 2026
Available online 19 June 2026

protection, and cybersecurity regulations, such as the Resilience of the Critical Entities Directive (EU) 2022/2557, NIS2 Directive (EU) 2022/2555, and the Chemical Weapons Convention (CWC). This fragmented landscape has produced distinct risk rationalities: safety emphasizes openness, transparency, and risk control, whereas security prioritizes confidentiality, controlled information flows, and threat prevention (Ab Rahim et al., 2025; Hansen and Antonsen, 2024; Ylönen et al., 2022).

Over time, these differing logics have reinforced structural and cultural fragmentation between safety and security (Glesner et al., 2022). Safety management relies on open reporting, trust, information sharing, and collaborative learning to maintain high reliability and detect weak signals. Security systems, by contrast, operate through rigid rules, restricted access, need-to-know principles, and coercive authority, limiting discretion and information flows (Glesner et al., 2022; Pettersen and Bjørnskau, 2015; Reniers et al., 2011). Consequently, organizations often maintain separate reporting channels, independent risk assessments, and parallel procedures, with some security measures hampering communication essential for safety (Pettersen and Bjørnskau, 2015). These divergent principles generate conflicting priorities. For example, safety's reliance on transparency and movement flexibility versus security's emphasis on confidentiality, standardization, and movement restriction (Glesner et al., 2022). Moreover, as Leveson (2020) notes, this separation is historically constructed rather than inherent; through a systems-theoretic perspective, safety and security address the same hazardous system states, meaning weaknesses in one domain can amplify vulnerabilities in the other.

Recent events underscore the consequences of this fragmentation. The 2013 In Amenas gas plant attack, the 2015 Tianjin port explosions, and the 2017 Triton malware incident demonstrated how weaknesses at the safety–security interface may escalate into systemic failures with catastrophic consequences (Casson Moreno et al., 2018; Iaiani et al., 2021; Yuan et al., 2024). These incidents illustrate how accidental and intentional risks propagate through shared infrastructures, human resources, and digital networks. Without an integrative perspective, such interdependencies remain hidden, limiting organizations' ability to holistically manage complex disruptions (Ab Rahim et al., 2025; Yang et al., 2023).

Resilience engineering has emerged as a promising paradigm to bridge these perspectives. Grounded in systems thinking, resilience engineering focuses on the ability of socio-technical systems to sustain essential functions under stress (Hollnagel, 2006; Pasman et al., 2020). However, resilience is not a universal or static concept; as Mentges et al. (2023) emphasize, definitions of resilience vary across domains and must be adapted to the characteristics, functions, and stressors of the system under consideration. In critical infrastructures such as the CPI, resilience spans multiple dimensions, i.e., technical, organizational, social, and economic. They connect the robustness of physical systems with the organizational capacities required for adaptation, decision-making, and governance. Although recent studies highlight resilience as a way to strengthen the ability of process plants and organizations to anticipate, absorb, adapt to, and recover from disruptions (Geng et al., 2023; Zeng et al., 2025; Zinetullina et al., 2021), empirical tools that translate these principles into integrated safety–security management remain limited (Jovanović et al., 2018; Pasman and Rogers, 2014).

Despite growing interest, several gaps persist. First, fragmentation between safety and security risk management continues to limit systemic understanding of industrial risk. Second, although the broader need to integrate safety and security is increasingly recognized, such integration remains less developed when approached through a resilience engineering paradigm tailored to the CPI. Third, resilience principles are rarely translated into practical management structures, performance indicators, and learning mechanisms that enable cross-boundary coordination and long-term improvement. Existing risk management methods and performance indicators remain discipline-specific, obscuring the dual nature of safety–security disruptions and the capacities required to manage them (Bischoff et al., 2015; Pettersen Gould and Bieder, 2020; Reniers et al., 2020; Ylönen et al., 2022). Within this broader research program, the present study builds on earlier review-based and survey-based work and forms the framework-development stage that precedes subsequent industrial application, as summarized in Fig. 1.

This paper addresses these gaps by developing the Resilience-oriented Process Safety and Process Security (RoPSS) as an expert-informed conceptual framework designed for operationalization. The paper contributes by: (i) integrating process safety and process security through a resilience-oriented framework; (ii) introducing Ascension as an evolutionary resilience capability that consolidates recovery, learning, continuous improvement, and prevention into a single forward-looking function that reconnects operational practice with organizational governance; (iii) translating this logic into a six-step management cycle; and (iv) developing a corresponding performance indicator architecture to support future operationalization.

The remainder of this paper is organized as follows. Section 2 presents the conceptual foundations of unified risk management, coupled safety–security dynamics, resilience capabilities, and performance measurement. Section 3 describes the research design and expert interviews and elicitation process. Section 4 presents the results, including the six-step RoPSS framework, the resilience-oriented indicator catalogue, the importance–availability assessment, and an illustrative example. Section 5 discusses the conceptual, practical, and methodological implications. Section 6 concludes with recommendations and directions for future research.

2. Literature and theoretical construct

2.1. Resilience as a systemic risk management paradigm

Modern chemical process facilities operate as tightly coupled socio-technical systems in which technical components, digital controls, and human–organizational factors continuously interact (Pasman et al., 2020; Rasmussen, 1997). Within such complexity, accidents and intentional disruptions share many causal pathways. For instance, a cyber intrusion may disable the same control logic that fails during a process upset, while a maintenance lapse may create vulnerabilities exploitable by sabotage (Ab Rahim et al., 2025). As Aven (2007) argues, intentional and unintentional disruptions differ mainly in their origin rather than in their analytical structure; both involve sources, vulnerabilities, potential consequences, and associated uncertainties. More recent risk scholarship further cautions against treating risk and resilience as disjoint concepts, emphasizing that resilience assessment and management should consider potential events, consequences, uncertainties, and recovery processes (Aven, 2022). These interdependencies indicate that process safety and process security are not parallel disciplines but coupled subsystems within a broader system of systemic risk (Glesner et al., 2022). Managing these interactions requires a paradigm capable of sustaining essential functions across varying and unforeseen conditions rather than focusing solely on the prevention of individual failure modes (Ab Rahim et al., 2024; Yarveisy et al., 2022).

Resilience engineering provides such a paradigm. Emerging from safety science and systems theory, resilience engineering reframes risk management from preventing deviation to sustaining performance under disturbance (Hollnagel, 2006; Jain et al., 2020; Woods, 2015). Rather than focusing solely on preventing specific failure modes, resilience engineering emphasizes a system's ability to continue functioning under varying and unexpected conditions (Hosseini et al., 2016; Pawar et al., 2021). In this perspective, safety and security are not viewed as end states but as dynamic properties of a system that adapts, recovers, and learns in the face of uncertainty (Yang et al., 2023). In contrast to traditional quantitative risk assessment tools such as fault tree or event tree analysis, which model predefined sequences of failure, the

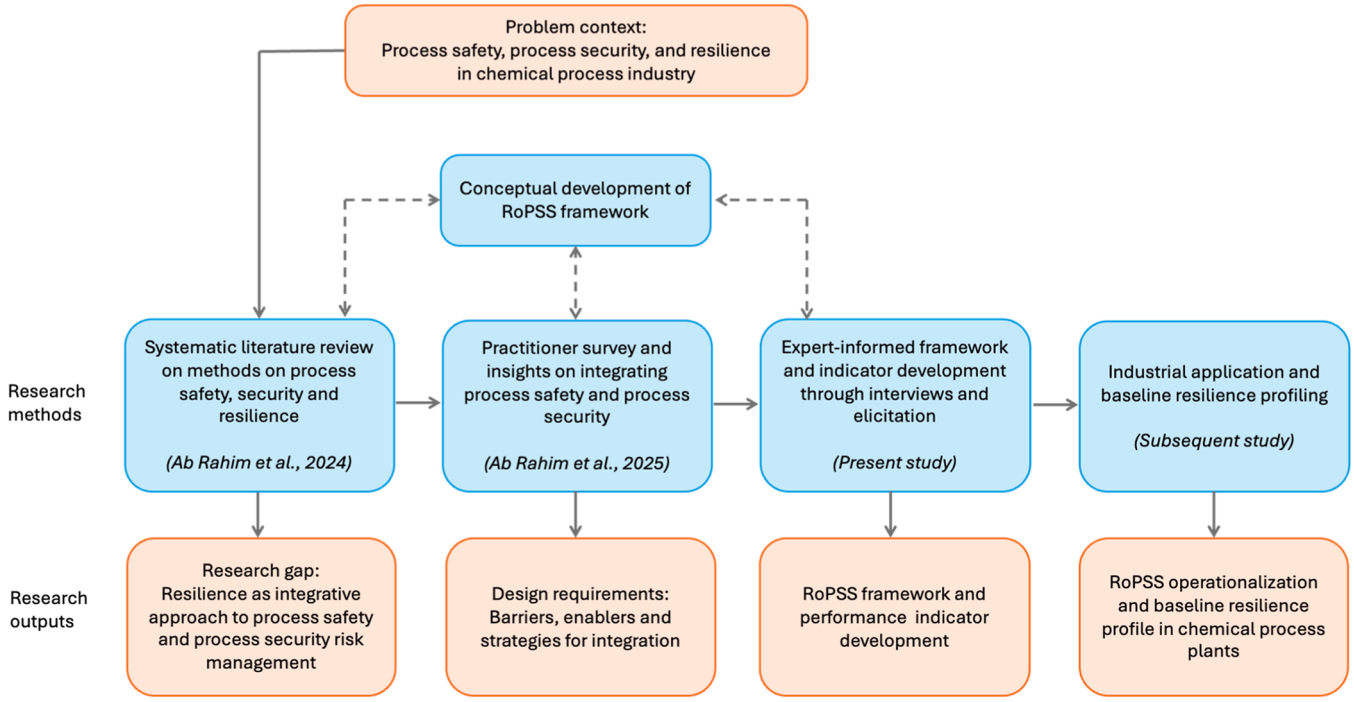

Fig. 1. Research roadmap showing the development of the RoPSS framework within the broader research program.

resilience perspective acknowledges the emergent and non-linear nature of socio-technical performance variability (Ab Rahim et al., 2024). This broader understanding of resilience is reflected in Ayyub (2014):

> *"Resilience notionally means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from disturbances of the deliberate-attack types, accidents, or naturally occurring threats or incidents. The resilience of a system's function can be measured based on the persistence of a corresponding functional performance under uncertainty in the face of disturbances."*

Ayyub's definition is particularly relevant for the CPI, where facilities face both accidental disruptions (e.g., equipment failures, human errors) and intentional threats (e.g., sabotage, cyberattacks) (Ab Rahim et al., 2025; Yang et al., 2023; Yuan et al., 2024). Increasing digitalization and automation have intensified the coupling between safety-critical and security-critical systems, as sensors, programmable logic controllers, and remote monitoring networks now mediate both operational reliability and defensive integrity (Landucci et al., 2020; Yuan et al., 2024; Zhang et al., 2024). Consequently, risk management in the CPI must address system performance continuity rather than discrete hazard categories.

Conceptually, resilience engineering is grounded in Hollnagel's four cornerstones — anticipate, monitor, respond, and learn — which describe how socio-technical systems maintain performance amidst variability and uncertainty (Hollnagel, 2006). These functions remain foundational to the proposed framework but are reorganized into four resilience capabilities, namely Anticipation, Absorption, Adaptation, and Ascension, that together define how organizations sustain essential functions under both accidental and deliberate disruptions. Ascension, as elaborated later, consolidates recovery, learning, continuous improvement, and prevention into a single long-term capability.

Within this systemic view, resilience functions as a unifying management logic that aligns preventive and protective actions across technical, human, and organizational layers (Jain et al., 2018; Pasman et al., 2020). It connects process safety and process security objectives within a single dynamic management framework, one that values flexibility, feedback, and continuous improvement as much as barrier robustness or procedural compliance (Linkov, 2019). These conceptual foundations provide the operational basis for the capability-based interpretation of resilience developed in the following sections. By positioning resilience as a systemic paradigm, this study establishes the conceptual foundation for the RoPSS framework. The next subsection elaborates on how safety and security interact within such socio-technical systems, forming coupled dynamics whose management depends on these resilience capabilities.

2.2. *Coupled process safety–security dynamics in socio-technical systems*

Within the systemic paradigm described above, process safety and process security are dynamically coupled through shared technologies, infrastructures, and human activities. In modern process facilities, many physical and organizational controls, such as access management, alarm systems, control room operations, and maintenance procedures, serve both safety and security functions (CCPS, 2022). As a result, actions designed to strengthen one dimension may inadvertently influence the other, either positively or negatively (Pettersen and Bjørnskau, 2015). These interdependencies create a coupled risk system in which failures, adaptations, and improvements propagate across domains rather than remaining confined within them (Kenneth and Gould, 2020; Leveson, 2020). Recent methodological studies reinforce this integrated view, including Bayesian-network-based modelling of intentional and unintentional causation pathways (Amin et al., 2022) and dynamic risk assessment of chemical industry park cyber-physical systems using coupled safety and security risk indicators (Huang et al., 2025).

Coupling in industrial operations can range from loose to tight interactions (Perrow, 1999). Loose coupling allows local flexibility and buffering between safety and security processes, whereas tight coupling means that a single event, such as a cyber intrusion, valve malfunction, or operator error, can simultaneously degrade protective barriers and expose security vulnerabilities (Kenneth and Gould, 2020; Perrow, 1999). Chemical plants increasingly operate under tightly interconnected conditions due to digitalization, just-in-time supply chains, and shared human-machine interfaces (Zhang et al., 2024). In such environments, resilience depends less on the strength of individual barriers than on an organization's capacity to sense, interpret, and

respond to cross-domain interactions that cut across disciplinary and functional boundaries (Patriarca et al., 2018).

As systems become more integrated, trade-offs between safety and security objectives also become more apparent. Examples include tension between evacuation and lockdown decisions during emergencies, or between transparency and confidentiality in incident reporting and information sharing (Glesner et al., 2022). Findings from the practitioner survey reported in Ab Rahim et al. (2025) reinforce this observation. Although 72 % of respondents acknowledged the benefit of integration, many also highlighted persistent obstacles such as siloed communication, unequal resource allocation, and unclear leadership responsibilities. These challenges indicate that coupling is not solely technical but also socio-organizational, shaped by institutional priorities and professional cultures.

Understanding these coupled dynamics is central to advancing a resilience-oriented approach to risk management in the CPI. Resilience provides the theoretical and practical mechanisms by which organizations anticipate, absorb, adapt to, and learn from disturbances that cross safety–security boundaries. In this context, safety and security no longer function as separate control loops but as interdependent feedback systems linked by shared information flows, resources, and decision hierarchies (Blokland and Reniers, 2020; Schulman, 2020). Managing such coupling, therefore, requires organizational capabilities that maintain functional balance and adaptability without undermining either domain.

2.3. Resilience capabilities and the evolutionary role of ascension

The literature on critical infrastructures and process industries commonly operationalizes resilience through a set of capabilities that describe system behavior before, during, and after disruption. Most resilience engineering models include anticipation, absorption, adaptation, and restoration, which together explain how organizations prepare for, withstand, and recover from disturbances of various origins (Geng et al., 2023; Mentges et al., 2023; Yang et al., 2023; Yarveisy et al., 2020). These capabilities provide a structured lens for analyzing performance dynamics and organizational learning across the life cycle of disruptions, encompassing both process safety and process security perspectives.

Hollnagel's four cornerstones remain foundational to the resilience engineering paradigm, describing how socio-technical systems manage performance variability and feedback across human, technical, and organizational layers (Hollnagel, 2006; Yarveisy et al., 2022). Vert et al. (2021) further distinguish adaptive capacity (i.e., the enabling mechanisms such as sensemaking, monitoring, coordination, and learning) from adaptation (i.e., the actual modification of structure or behavior in response to adversity). This distinction clarifies how resilience emerges from the interaction of human cognition and organizational coordination within safety- and security-critical socio-technical systems.

Across these perspectives, four core capabilities capture the temporal and functional dynamics of resilience. *Anticipation* refers to the proactive capacity to detect weak signals, monitor emerging threats, and prepare for potential disruptions before they escalate. It involves activities such as systematic risk assessment, early warning, resource planning, and competency development (Geng et al., 2023; Mentges et al., 2023). In a coupled safety–security context, anticipation includes identifying how hazards and threats may interact. For example, how a maintenance failure could be exploited through cyber intrusion, or how security restrictions might delay safe evacuation (CCPS, 2022; Pettersen and Bjørnskau, 2015).

Absorption denotes the system's ability to withstand shocks and minimize performance degradation during disruptions. This capability relies on robustness, redundancy, and buffering mechanisms that preserve critical functions during stress (Mentges et al., 2023; Yang et al., 2023). Examples include the availability of standby utilities, safety interlocks, or containment barriers that limit both accidental releases and deliberate tampering. In resilience terms, absorption represents the immediate defensive posture that prevents cascading losses while maintaining essential operations (Geng et al., 2023).

Adaptation encompasses the dynamic capacity to reconfigure processes, procedures, and resources as conditions evolve. It reflects the flexibility of human and organizational systems to coordinate under pressure, make trade-offs, and adjust behaviors when predefined procedures are insufficient (Mentges et al., 2023; Patriarca et al., 2018). In practice, adaptation enables integrated responses under coupled safety–security scenarios, such as balancing evacuation and lockdown decisions or reallocating personnel between emergency and protection functions (Ab Rahim et al., 2025).

Restoration concerns the ability of a system to re-establish and stabilize performance following a disturbance. It includes physical repair, reinstatement of normal operations, and verification of system integrity after the acute response phase (Geng et al., 2023; Mentges et al., 2023; Yarveisy et al., 2020). Restoration thus forms the bridge between short-term absorption and long-term recovery, representing the stage at which a system seeks to return to an acceptable performance level (Tong et al., 2020; Yarveisy et al., 2022).

Yarveisy et al. (2020) conceptualized these interrelations through absorptive, adaptive, and restorative capacities (Fig. 2). While such models capture the essential before–during–after sequence of resilience, most conclude at the restoration phase (Geng et al., 2023). Other scholars have emphasized that resilience should also encompass what happens after recovery, namely how organizations learn, improve, and prevent future failures (Mentges et al., 2023; Patriarca et al., 2018; Vert et al., 2021; Zeng et al., 2025).

Building on this progression, the present study introduces *Ascension* as an evolutionary capability. Within the proposed framework, Ascension functions as a unifying capability that integrates restoration (recovery), learning, continuous improvement, and prevention into a coherent trajectory of system evolution. Rather than redefining resilience, Ascension extends existing models by emphasizing that resilience includes not only the capacity to respond and recover, but also the capacity to evolve and strengthen through accumulated experience. It represents the feedback mechanism that links operational resilience with organizational and governance resilience. Ascension embeds principles of double-loop learning, preventive redesign, and cross-domain knowledge transfer, enabling improvements that span both

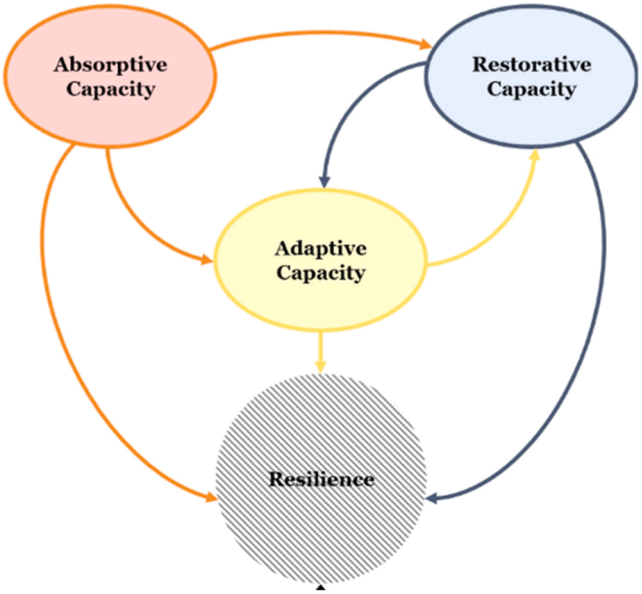

Fig. 2. Logical relation of system capacities with resilience (adopted from Yarveisy et al., 2020).

process safety and process security. Through this capability, resilience becomes progressive rather than merely cyclical, characterized by continuous refinement of functions, coordination, and foresight.

This broader interpretation is important for integrated process safety and process security because coupled disruptions often require coordination across operations, safety, security, maintenance, management, and external stakeholders (Hansen and Antonsen, 2024; OECD, 2019). The RoPSS framework therefore links operational response with governance-level learning through its six-step management cycle and the Ascension capability.

2.4. Resilience measurement and performance indicators

Quantifying resilience has long been a challenge in managing complex socio-technical systems. By contrast, performance indicators have a long history in process safety management and are widely used to monitor compliance, critical activities, and safety outcomes (HSE UK, 2006; Swuste et al., 2016). However, traditional indicators in the CPI were developed for discipline-specific objectives, primarily focusing on process safety, with far less systematic attention to process security (Khan et al., 2010). Existing systems also tend to prioritize lagging outcomes and monitor safety and security through separate metrics and reporting channels (Reniers et al., 2011; Sultana et al., 2019; Swuste et al., 2016). This separation limits visibility of interdependencies and constrains proactive learning across domains. Translating resilience capabilities into measurable indicators therefore offers a practical pathway for connecting operational performance, organizational preparedness, and governance-level learning within a unified resilience-oriented framework for process safety and process security (Ab Rahim et al., 2025; Leveson, 2015; Pasman and Rogers, 2014; Yarveisy et al., 2022).

Resilience measurement must capture not only operational performance but also the governance processes that sustain learning and adaptation. Indicators, therefore, act as a bridge between day-to-day management and organizational resilience (Pasman and Rogers, 2014). Recent research highlights indicator- and index-based approaches as useful semi-quantitative tools when probabilistic data are limited (Hosseini et al., 2016; Yarveisy et al., 2022). Yet many of these methods still focus mainly on absorption and recovery, overlooking anticipatory and learning capacities. The present study advances a more balanced approach by mapping indicators across all four resilience capabilities, thereby extending performance measurement from preparedness to continuous improvement.

The development of performance indicators for process safety has evolved over several decades. The UK Health and Safety Executive's guidance on *Developing Process Safety Indicators* (HSE UK, 2006) introduced the concept of *dual assurance* through combined leading and lagging indicators. Leading indicators provide proactive checks on safety-critical activities and barriers, whereas lagging indicators reveal the deterioration or failures of those barriers. This dual-layer structure has influenced later frameworks such as the OECD Guidance on Developing Safety Performance Indicators for Industry, Public Authorities and Communities (OECD, 2008a, 2008b), and the American Petroleum Institute (API) Recommended Practice 754 on Process Safety Performance Indicators for the Refining and Petrochemical Industries (API, 2021). API RP 754, for example, classifies indicators into four tiers ranging from major consequence events to early operational deviations (API, 2021; Khan et al., 2010).

At the regulatory level, the EU Seveso III Directive requires operators to maintain comprehensive safety management systems, monitor performance, and engage with stakeholders. The updated OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response (OECD, 2023) further emphasize governance mechanisms for addressing multi-hazard scenarios, including domino effects, cyberattacks, and Natech events, by promoting performance measurement and continuous improvement across all levels of governance. These developments have progressively transformed indicators from compliance-based control tools toward more strategic instruments that reflect system capability and learning potential (Leveson, 2015). Within a resilience engineering context, indicators represent signals of a system's capacity to anticipate, absorb, adapt, and ascend through disruption. When shared across safety and security functions, they support more unified decision-making and strengthen the basis for integrated resilience management (Jovanović et al., 2018).

Performance indicators can also support barrier-based risk management by tracking whether preventive and mitigative barriers remain available, reliable, tested, and improved over time. This is consistent with the "As Low As Reasonably Practicable" (ALARP) approach, which requires risk controls to remain effective and to be further improved where reasonably practicable (CCPS, 2022). Recent resilience assessment work similarly emphasizes the role of system dynamics and Independent Protection Layers (IPLs), including basic process control, alarms, safety instrumented systems, and pressure relief devices, in evaluating chemical process system responses under disruption (Sun et al., 2025). In this regard, BowTie analysis and Layer of Protection Analysis (LOPA) can help visualize accident and threat pathways, while resilience-oriented indicators support ongoing review of the associated barriers. This is particularly relevant for integrated process safety and process security, where barriers such as access control, alarm management, emergency shutdown, containment, and cybersecurity protection may influence both accidental and intentional risk pathways.

Building on this lineage, the present study extends indicator logic into a resilience-oriented paradigm that addresses both process safety and process security dimensions. Following Meyer and Reniers (2022), these resilience capabilities are operationalized through three interrelated types of indicators:

i. *Management indicators* are proactive (leading) and address the question "With what means?" They evaluate resources, competencies, and organizational mechanisms that mainly support preparedness and Anticipation.
ii. *Process indicators* are also proactive, focusing on "How" effectively operational systems perform under both normal and disturbed conditions. They primarily support Absorption and Adaptation.
iii. *Result indicators* are more reactive (lagging) and address "What was achieved?" They capture recovery outcomes, post-event learning, and the integration of lessons into continuous improvement processes, thereby reflecting Ascension.

Together, these indicator types operationalize the four resilience capabilities within the proposed framework. Unlike conventional leading–lagging systems that often treat safety and security separately, this tri-dimensional typology integrates them across proactive, reactive, and evolutionary perspectives. Resilience-oriented indicators should also meet the SMART criteria (i.e., Specific, Measurable, Achievable, Relevant, and Time-bound), while addressing both safety and security concerns (Meyer and Reniers, 2022). When designed accordingly, they serve as measurable connectors between risk management, operational control, and governance learning.

2.5. Conceptual integration towards a resilience-oriented framework

The preceding discussion establishes resilience as a systemic paradigm that unites operational, organizational, and governance dimensions of risk management. Over the past decade, several scholars have advanced this understanding by formalizing resilience as a measurable property of complex socio-technical systems. (Leveson, 2015) and (Sultana et al., 2019), for example, emphasized indicator- and index-based methods for managing uncertainty, while (Zio, 2018) proposed integrating resilience, adaptability, and sustainability in the governance of engineered systems under deep uncertainty. Quantitative

models developed by Yarveisy et al. (2020), Geng et al. (2023), and Yang et al. (2023) describe resilience through the temporal interplay of anticipation, absorption, adaptation, and restoration, framing it as a dynamic function of performance over time. Taken together, these studies provide a foundation for extending resilience from an operational concept to a more integrated management perspective relevant for both process safety and process security.

The CPI is exposed to various disruptions that may affect process safety and process security simultaneously. In line with Yang et al. (2023), who characterized resilience through the triplet relation of disruption, functionality, and performance, the present study adopts a systemic perspective to connect potential disturbances with organizational responses across both domains. Yang et al. (2023) distinguish between internal disruptions (e.g., technical failures, human errors, and managerial deficiencies) and external disruptions (e.g., natural disasters, social hazards, and terrorism). This taxonomy offers a structured basis for identifying potential disturbance sources that affect system functionality and performance.

Building upon this logic, the present study refines the classification to eight disruption types: four internal and four external (Fig. 3). This typology broadens the scope of resilience assessment by capturing operational and socio-organizational stressors relevant to both process safety and process security in the CPI. Mapping disruptions across both domains encourages a holistic understanding of risk interdependencies and supports integrated approaches to preparedness, response, and long-term improvement.

Together, these theoretical developments form the conceptual foundation of the present study. Although process safety and process security share overarching goals, their methods, indicators, and governance structures often remain compartmentalized. A resilience-oriented approach provides a unifying paradigm by linking the proactive anticipation of disruptions, the ability to absorb and adapt under stress, and the capacity to learn and improve afterward. In this sense, the present study positions safety and security as complementary subsystems within a shared resilience engineering perspective.

Fig. 4 depicts how the four resilience capabilities function as a continuous management cycle connecting operational performance with organizational governance. Indicators within the process safety and process security circles represent domain-specific operational measures, while those in the overlapping region capture cross-domain interactions

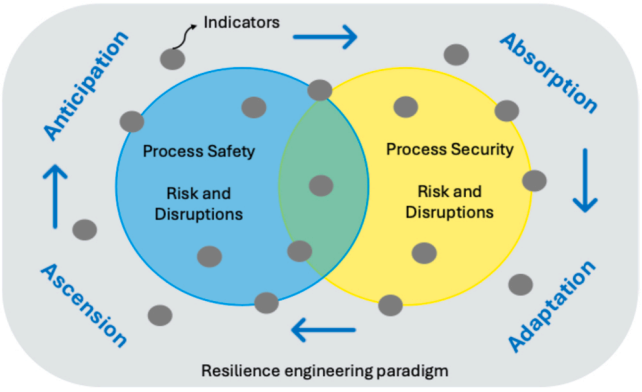

Fig. 4. Conceptual integration of process safety and process security within the resilience engineering paradigm. The four resilience capabilities form a continuous cycle through which indicators bridge risk and disruption management across both domains.

such as shared disruptions, coupled system behaviors, and joint responses. Indicators located outside the circles denote governance-level functions supporting strategic oversight, resource allocation, institutional learning, and long-term priority setting. Ascension acts as the feedback mechanism through which insights from operational and governance indicators inform preventive action, policy revision, and system-wide improvement. Within this paradigm, indicators collectively translate resilience principles into both operational practice and governance processes. By combining the disruption classification, resilience capabilities, and indicator typology, this conceptual synthesis provides the basis for developing the integrated framework.

3. Methodology

3.1. Research design and rationale

This study adopts a mixed-methods design that combines prior empirical work, conceptual development, and expert elicitation to develop the RoPSS framework. As Creswell (2018) explains, mixed-methods research combines quantitative breadth with qualitative

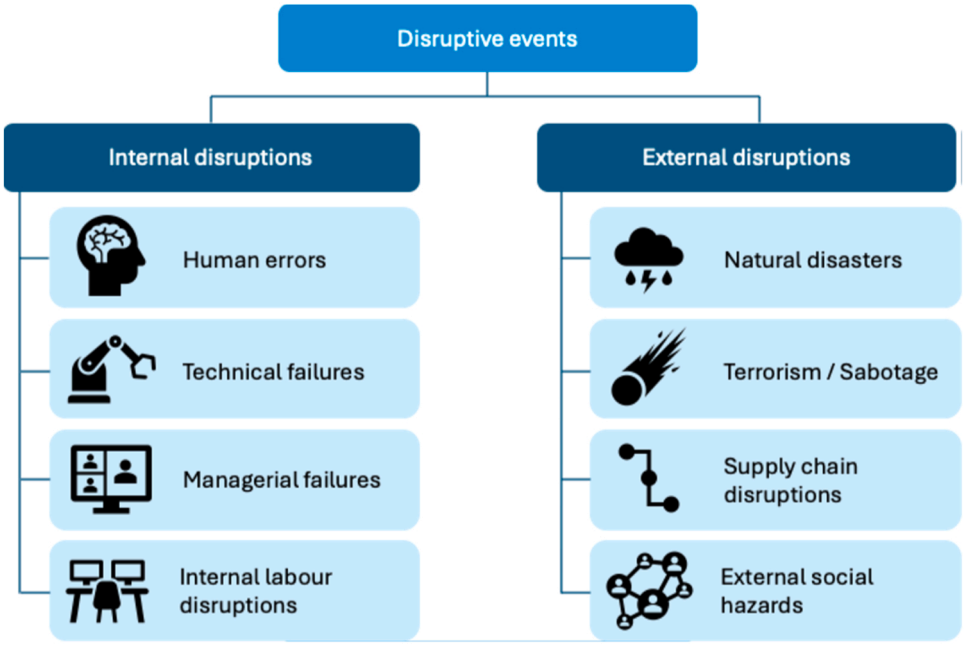

Fig. 3. Classification of disruptive events encompasses eight disruption types (four internal and four external).

depth to achieve a more comprehensive understanding of complex phenomena. In this present study, prior empirical findings are expanded and contextualized through new qualitative insights. The research process unfolded through four iterative stages as below:

i. **Foundational synthesis from authors' prior work**: (Ab Rahim et al., 2024) provided a systematic literature review of risk assessment methods for process safety, process security, and resilience, identifying methodological fragmentation and conceptual gaps. Subsequently, (Ab Rahim et al., 2025) contributed empirical evidence through a practitioner survey, revealing the needs, barriers, and enablers for the integration.
ii. **Targeted literature enrichment:** For the present study, additional literature focusing on resilience engineering, performance-indicator frameworks, and governance integration, as discussed in Section 2, was reviewed to complement these earlier foundations.
iii. **Expert interviews with scenario-based elicitation:** Semi-structured interviews were conducted with domain experts to refine the structure of the RoPSS framework, its resilience capabilities, and the draft performance indicator catalogue through discussion of disruption scenarios and integration challenges.
iv. **Indicator importance–availability assessment through focused expert elicitation:** A subset of experts participated in a rating exercise to assess each draft indicator in terms of its importance for integrated risk management and the availability of supporting data. The results informed the refinement, prioritization, and consolidation of the indicator catalogue.

3.2. Semi-structured interviews and scenario-based elicitation

Data were collected through semi-structured interviews with 16 purposively selected experts to represent diverse professional backgrounds (Table 1): industry practitioners (n = 8), consultants (n = 2), government experts (n = 4), and academics (n = 2). This diversity was essential to capture operational, regulatory, and conceptual perspectives on process safety and process security integration. All participants provided informed consent, and identifiers were anonymized to maintain confidentiality.

Interviews followed a flexible guide, allowing interviewees to speak freely and fully (Magnusson and Marecek, 2015), and covering six thematic areas: (i) professional background and role; (ii) perceived benefits of integrating process safety and security; (iii) challenges and barriers to integration; (iv) views on the applicability of resilience concepts; (v) recommendations for effective integration; and (vi) suggested performance indicators for managing process-safety and process-security risks. Working definitions of key concepts were provided to ensure common understanding across informants.

Within these interviews, a scenario-based elicitation technique (Schoemaker, 1993) was embedded to stimulate reflection. Eight disruption scenarios were used: human error, technical failure, managerial failure, internal labor disruption, natural disasters, terrorism/sabotage, supply-chain disruption, and external social hazards. Each scenario highlighted both safety and security implications, prompting experts to discuss how system function objectives, resilience capabilities, and indicators would perform under such conditions. Embedding these scenarios into the interviews help ground responses in operational reality and supported the development of a framework applicable across diverse disruption types. To accommodate time constraints and domain expertise, participants chose one or more scenarios most relevant to their background. On average, each interview session lasted around 82 min. Although all six thematic areas were explored, the present paper focuses on the interview findings directly relevant to the development and refinement of the resilience-oriented framework and its performance indicators. The selection process for both the semi-structured interviews and the subsequent focused expert elicitation

Table 1
Summary of interviewees by sector, position, experience, and expertise.

ID	Sector	Position	Experience	Expertise
A01	Academia	Professor	30 + years	Process safety management expertise and industry consultant
A02	Academia	Associate Professor	25 + years	Process safety and chemical engineering expertise; former industrial professional
C01	Consultant	Industrial Major Hazard Competent Person	20 + years	Process safety management and consultancy in multinational operations
C02	Consultant	Business Consulting Manager	20 + years	Business operations and supply chain in the chemical-related industry
G01	Government	Director of Chemical Security Authority	20 + years	Policy development and enforcement in chemical security and chemical management
G02	Government	Deputy Director of Industrial Major Hazard Section	15 + years	Policy development and enforcement of process safety and security for major hazard installations
G03	Government	Assistant Director of Petroleum Safety Division	10 + years	Enforcement of process safety and chemical disaster management
G04	Government	Assistant Director of Safety and Health Policy Division	10 + years	Policy development in chemical safety and security risk management
I01	Industry	Health and Safety Manager	30 + years	Process safety management in the chemical process industry
I02	Industry	Safety and Security Officer	30 + years	Safety and security risk management, with expertise in physical and cybersecurity
I03	Industry	Health and Safety Manager	30 + years	Safety management in major hazard installations and operations
I04	Industry	Supply Chain and Procurement Manager	20 + years	Supply chain and procurement management for chemical process plants operations
I05	Industry	Fire and Emergency Response Manager	20 + years	Firefighting and emergency response management in the chemical process industry
I06	Industry	Information and Cybersecurity Manager	15 + years	Cybersecurity and information management for chemical process plants operations
I07	Industry	Security and Human Resource Manager	15 + years	Human resources and physical security management in the chemical process plants
I08	Industry	Process Engineer	10 + years	Process hazard analysis and process control in the chemical process plants

for indicator refinement is summarized in Fig. 5.

3.3. Data analysis and coding

Interview transcripts and field notes were analyzed using thematic analysis (Braun and Clarke, 2006), and the Thematic Analysis Matrix (TAM) model developed by Zairul (2024). Coding was primarily inductive, allowing themes to emerge from the data, but was also informed deductively by the four resilience capabilities: Anticipation, Absorption, Adaptation, and Ascension. Codes were iteratively refined and grouped into higher-order categories representing resilience functions and integration strategies. These themes informed successive revisions of the indicator catalogue and helped ensure that indicators reflected the SMART criteria in ways applicable to both process safety and process security management contexts. Selected excerpts from the interviews are presented in Section 4 to illustrate key findings.

This analytic process also informed the development of the initial set of 70 performance indicators, which emerged through an iterative, researcher-led synthesis grounded in multiple sources of evidence and expert input. Earlier stages of the study, including the literature review and practitioner survey, identified key integration challenges, resilience-related requirements, and measurement gaps in process safety and process security management. These inputs informed the conceptual development of the RoPSS framework, from which a preliminary set of candidate indicators was drafted by the researcher and iteratively discussed with the supervisory team. This preliminary set was then examined and refined through semi-structured expert interviews, during which interviewees suggested improvements, clarifications, and additional indicators across the eight disruption types and four resilience capabilities. The researcher subsequently consolidated these inputs into an initial draft catalogue of 70 indicators, intentionally broad in scope to ensure conceptual coverage before later refinement through focused expert elicitation and formative assessment.

3.4. Assessing indicator importance and availability

To support the practical refinement of this 70-indicator draft catalogue, a focused expert elicitation was subsequently conducted with four experts (two from industry and two from government), all with substantial experience in process safety and process security risk management. As shown in Fig. 5, these experts were selected from the broader pool of interview participants. This step was intended as a formative assessment to support indicator refinement and prioritization. Each expert rated the draft indicators on two dimensions, namely importance and data availability, using a five-point scale. Importance referred to the perceived relevance of an indicator for integrated process safety and process security risk management, while data availability referred to the perceived ease of obtaining the required information in practice. Qualitative comments were also recorded where needed to clarify ratings or identify feasibility concerns.

For each indicator, the ratings were aggregated using the mean score for each dimension. Indicators with a mean score of 3.0 or above were classified as high, while those with a mean score below 3.0 were classified as low. Based on these mean scores, the indicators were grouped into four quadrants in the importance–availability matrix. This appraisal was used to identify indicators that were both strategically relevant and practically measurable, as well as those that were important but more difficult to operationalize. The results informed the subsequent refinement of the indicator catalogue through consolidation, rewording, reclassification, and selective removal. Detailed indicator-level ratings and descriptive statistics are available in the associated public repository.

3.5. Trustworthiness and ethical considerations

Methodological trustworthiness was strengthened through triangulation across prior literature, practitioner survey findings, expert interviews, supervisory feedback, and iterative expert review of developing framework and indicator materials. In several cases, experts provided follow-up comments by email, which were reviewed and incorporated into subsequent refinements. Transparency was further supported through the public repository, which includes the full interview guide, consent template, integrated codebook, Thematic Analysis Matrices (TAMs) with illustrative quotations, and the expert elicitation dataset used for the formative assessment of indicators. This study was approved by the Human Research Ethics Committee of TU Delft on 17 January 2024 and complied with relevant research ethics requirements, including informed consent, anonymization, and secure data storage.

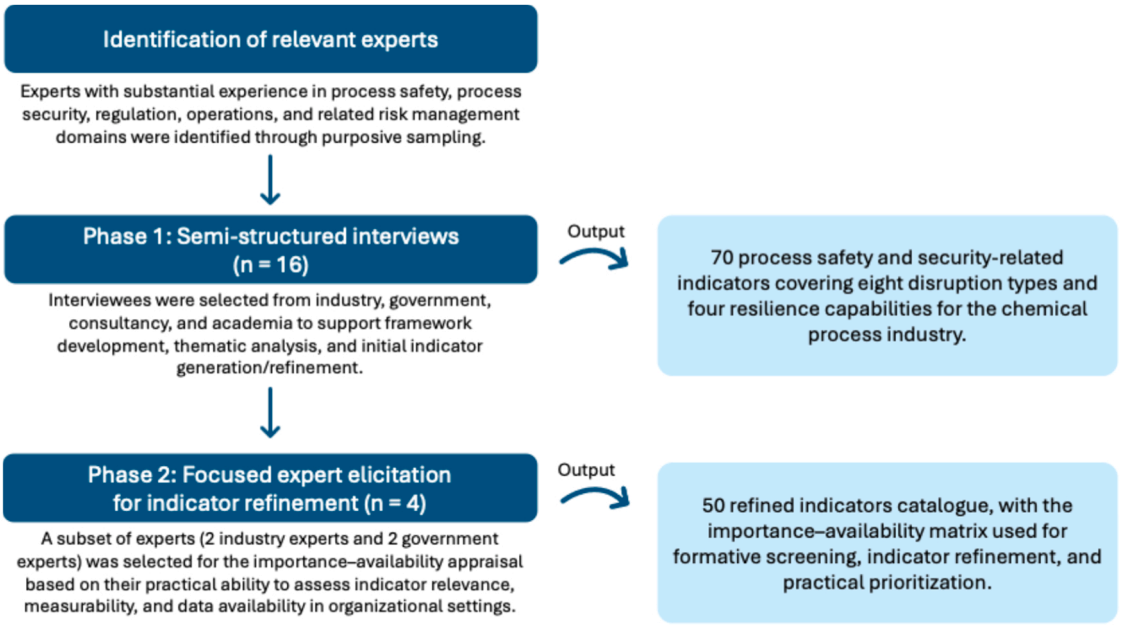

Fig. 5. Expert selection process for semi-structured interviews and focused expert elicitation for indicator development and refinement.

4. Results

4.1. Challenges and integration requirements

Expert interviews revealed five interrelated themes that constrain the integration of process safety and process security in the CPI. Together, they help explain why existing management approaches fall short of achieving resilience-oriented integration across systemic, coupled, and governance dimensions.

i. Organizational fragmentation and governance gaps

Safety and security functions are traditionally separated due to differing regulatory regimes, professional traditions, and technical expertise (Pettersen Gould and Bieder, 2020). Process safety evolved from industrial major accident prevention and engineering reliability, whereas (process) security stems from counterterrorism, physical protection, and cybersecurity. This separation offers benefits such as specialized expertise, clear accountability for legal compliance, and focused resource allocation. In many organizations, safety teams are situated within operations or HSE departments, whereas security is overseen by corporate security or IT governance (Glesner et al., 2022).

However, experts stressed that this separation creates overlaps, blind spots, and inconsistent priorities, particularly at the safety–security interface where both domains depend on shared control systems, data, and infrastructure. As one industry participant (I01) noted, *"Right now, safety and security teams hardly talk to each other."* Fragmentation diffuses accountability for cross-cutting risks and undermines coordination. Leadership gaps further reinforce this issue: as one consultant (C02) stated, *"Integration won't work if top management still sees safety and security as separate boxes."* Without clear mandates and cross-functional leadership, integration remains optional rather than strategic.

ii. Imbalanced and lagging measurement practices

Current performance measurement systems rely heavily on lagging indicators, such as lost-time injuries (LTI) and process safety event counts. By contrast, limited attention is given to proactive metrics that reflect organizational preparedness and system resilience. As one consultant (C01) explained, *"We rely too much on incident statistics; proactive measures are lacking."* This imbalance is driven by regulatory environments that emphasize retrospective reporting and compliance verification, reinforcing a reactive culture.

Although organizations collect potential leading indicators such as inspection compliance, training completion, and preventive maintenance budgets, these are often treated as administrative targets rather than as indicators of system health. Experts stressed that dual-purpose leading indicators, including near-miss reporting, cross-functional training, and joint safety–security audits, would allow earlier detection of deteriorating conditions and promote proactive decision making.

iii. Emerging cyber-physical vulnerabilities

Digitalization is creating stronger interdependencies between safety-critical and security-critical systems. Several experts warned that automation and connectivity blur the boundary between accidental and intentional failures. As one academic (A02) noted, *"Digitalization is creating new vulnerabilities that neither safety nor security fully covers."* Many organisations lack the analytical tools and data governance structures to assess these hybrid risks. Integrating cybersecurity with process safety management was viewed as essential to maintaining functional integrity and preventing cascading failures across interconnected systems (CCPS, 2022). Experts highlighted that the convergence of information technology (IT) and operational technology (OT) systems increases coupling across controls, alarms, authentication, and remote access, thereby requiring more integrated oversight.

iv. Resource and capacity constraints

Financial and human-resource limitations were also cited as barriers to integration. Budgets, staffing, and training programs are often designed for single-discipline compliance rather than dual-purpose resilience. One industry expert (I06) observed, *"Integration requires additional time and resources, which can be difficult to secure alongside existing commitments."* Limited investment in integrated monitoring tools, data infrastructure, and cross-disciplinary training constrains proactive coordination between safety and security functions and impedes long-term improvement efforts.

v. Weak learning and feedback mechanisms

Experts also identified shortcomings in post-event learning and feedback processes. Incident investigations commonly address immediate safety causes, but seldom examine the security dimensions. A regulator (G03) commented, *"After an accident we look at safety failures, but rarely at how security weaknesses may played a role."* This lack of integrated learning loops prevents the consolidation of lessons across domains and inhibits systemic improvement. Participants stressed that resilience requires not only recovery but also structured reflection, institutional learning, and cross-functional knowledge sharing.

These five themes form the analytical foundation for designing the proposed framework and prioritizing its performance indicators. They reaffirm the integration requirements identified in Ab Rahim et al. (2025) while clarifying some of the mechanisms that impede progress. Notably, weak learning processes highlight the need for resilience capabilities that extend beyond traditional before–during–after models. This insight underpins the introduction of Ascension, which emphasizes recovery, learning, continuous improvement, and prevention. It also reinforces the need for a unified framework in which safety and security are recognized as coupled subsystems shaped by shared human, technical, environmental, managerial, and increasingly digital factors.

4.2. Resilience capabilities reflected in expert insights

The expert interviews and scenario-based elicitation reinforced the relevance of the four resilience capabilities as core mechanisms through which organizations manage coupled safety–security disruptions. While Section 2.3 established these capabilities conceptually, the interview results illustrate how they manifest in practice, revealing both strengths and gaps in current organizational arrangements. These insights informed the operationalization of the capabilities and guided the design of the indicator catalogue.

4.2.1. Anticipation

Experts highlighted shortcomings in the early detection of emerging hazards and threats. Operational foresight is often constrained by limited cross-functional communication and fragmented monitoring systems. Several participants explained that maintenance issues, access-control failures, or abnormal system states are frequently detected within departmental boundaries but seldom interpreted jointly. As one industry expert (I08) remarked, *"Weak signals are there, but no one is connecting the dots."*

Scenario discussions demonstrated that anticipatory practices should consider both accidental and intentional pathways. Vulnerabilities such as unsecured remote access, outdated firmware, or poor housekeeping can simultaneously increase safety and security risks. Likewise, security restrictions such as badge access or contractor vetting may inadvertently affect safe evacuation or maintenance response times. These insights indicate that anticipation requires integrated risk assessment, early warning, and cross-domain sensemaking, all of which informed the development of proactive management and process indicators in the framework.

4.2.2. Absorption

Interviewees recognized that organizations often rely on robustness and redundancy within safety systems, yet equivalent attention to security-related absorptive capacity is less developed. Safety barriers such as interlocks, alarms, containment systems, and emergency shutdown procedures increasingly rely on digitally connected infrastructures, making them vulnerable to cyber-physical intrusion.

Experts noted that tight coupling between IT and OT systems reduces buffering capacity and increases the likelihood of cascading failures. A scenario frequently cited was a cyber intrusion disabling a safety-instrumented system, compromising both safety and security protections. One expert (I02) remarked, *"We have good safety barriers, but many of them rely on systems that the security team barely touches."* These observations indicate that absorptive capacity should address both accidental and intentional disruptions and be evaluated through indicators that reflect barrier integrity, redundancy, and cross-domain protective functions.

4.2.3. Adaptation

Adaptation emerged as a critical capability for managing evolving, ambiguous situations. Experts observed that existing emergency response systems are often optimized for process safety scenarios, such as chemical leaks, fires, or explosions, and may not adequately address security threats or cyber-physical incidents. Experts pointed to common tensions between evacuation and lockdown decisions, which require rapid trade-offs that balance safety and security objectives.

Several interviewees emphasized flexible coordination mechanisms, cross-training, and clear delegation of authority during crises. As one consultant (C01) stated, *"Real events don't follow the plan; teams need the flexibility to adjust in real time."* Scenario-based elicitation highlighted the need to reconfigure workflows, integrate cybersecurity actions into physical responses, and maintain communication under degraded conditions. These insights informed the design of indicators that measure responsiveness, decision agility, inter-team coordination, and the organization's capacity to adjust procedures during hybrid disruptions.

4.2.4. Ascension

Experts identified weak learning and fragmented feedback loops as major impediments to long-term improvement. Investigations often focus on immediate technical or behavioral causes within the safety domain, while security-related vulnerabilities such as access failures, information gaps, or phishing attempts are seldom included in root-cause analyses. A regulator (G04) summarized this gap: *"We may recover from incidents, but sometimes we don't learn across both domains."*

Participants also noted that improvements are usually localized, with limited mechanisms for transferring lessons across sites and departments. This constrains organizational and governance learning required for sustained resilience in tightly coupled systems. These concerns support the introduction of Ascension as a capability that integrates recovery, learning, continuous improvement, and prevention. Within the proposed framework, Ascension links operational experience to governance adaptation by ensuring that findings, performance data, and weak signals inform policy refinement, redesign of controls, training programs, and long-term resource planning.

Collectively, these insights illustrate how the four resilience capabilities operate within coupled process safety–security environments and identify practical gaps, particularly in anticipation and learning, that the framework addresses through a structured combination of resilience capabilities and a multi-level indicator system.

4.3. The Resilience-oriented process safety and security (RoPSS) framework

The six-step Resilience-oriented Process Safety and Security (RoPSS) framework was developed as a practical management cycle to operationalize resilience and address the integration challenges identified by experts. It translates Anticipation, Absorption, Adaptation, and Ascension into concrete managerial practices that guide integrated process safety and process security management. The framework addresses practitioner-identified challenges, providing a resilience-oriented structure for managing coupled safety-security risks in the CPI.

4.3.1. Step 1 – Define the system

Experts stressed that clarity regarding scope, system boundaries, constraints, and stakeholder roles is essential to avoid accountability gaps. As one industry expert (I07) stated, *"If we do not clearly define who owns which responsibilities, especially between safety and security, things fall through the cracks."* A regulator (G01) added, *"Usually, safety talks to safety and security talks to security. We need a platform that forces them to sit at the same table."*

This step addresses siloed responsibilities by ensuring leadership and governance structures support integration. Practical examples include establishing a joint Safety–Security Interface Register and forming an Integrated Risk Management Committee to review shared controls. System definition is foundational for governance-level resilience as it creates shared ownership and transparency from the outset.

4.3.2. Step 2 – Identify disruptions

A recurring challenge was the fragmented assessment of accidental and intentional threats. Interviewees emphasized the need to systematically map disruptions that may affect process safety and process security. A consultant (C01) noted, *"A technical failure can easily trigger a security risk. For instance, if an alarm is down, it opens up an opportunity for malicious action."* An academic (A02) reinforced this view: *"We always prepare for accidents, but far less for deliberate acts. Hazards and threats can be mapped together."*

This step encourages a joint hazard-threat identification process that includes the eight disruption categories outlined earlier. For example, safety engineers and cybersecurity specialists may jointly assess how a control-system failure may stem from software errors (unintentional cause) or malware (deliberate attack). Similarly, supply chain managers and process engineers can evaluate risks related to counterfeit components or tampered deliveries alongside traditional safety concerns such as material incompatibility. Mapping disruptions through a systemic lens reflects the coupled nature of modern process systems and highlights common human, technical, and managerial factors influencing both safety and security outcomes.

4.3.3. Step 3 – Set system function objectives

Experts highlighted the difficulty of balancing competing values in process safety and process security management, particularly when objectives are set from a single-domain perspective. A consultant (C02) reflected, "*Sometimes we face dilemmas like whether to evacuate or lock down. Clear shared objectives help us manage those trade-offs*." A regulator (G02) added, *"When objectives are set only from a safety perspective, security suffers, and vice versa. We need a shared language of goals."*

This step translates the plant's mission and resilience priorities into measurable, mutually reinforcing objectives for process safety and process security. These objectives are aligned with the four resilience capabilities to ensure balanced attention to preparedness, response, recovery, and learning. Examples include:

i. **Anticipation:** Ensure that safety and security risk assessments are jointly conducted and periodically reviewed.
ii. **Absorption:** Implement redundant safety and security systems that can limit the impact of disruptions such as technical failures.
iii. **Adaptation:** Maintain proactive and corrective maintenance programs for safety- and security-critical equipment.
iv. **Ascension:** Integrate lessons learned from incidents or near misses into operational practices to support continuous improvement.

4.3.4. Step 4 – Set performance indicators

Experts identified the lack of proactive and dual-purpose indicators as a major shortcoming. One academic (A01) noted, *"We already track incidents, but that is history. What we lack are proactive indicators that show if we are truly ready."* A consultant (C01) emphasized, *"Security KPIs rarely align with safety KPIs. If indicators are designed together, they can drive real integration."* Participants also noted that resource constraints require concise and feasible indicator sets.

This step addresses fragmented measurement by establishing a structured catalogue of management, process, and result indicators that are concise and SMART. Examples include:

i. **Management indicator:** Percentage of annual budget allocated to non-hardware safety and security initiatives (training, risk assessment, investigation quality).
ii. **Process indicator:** Proportion of safety- and security-critical equipment with secondary containment systems installed and functioning.
iii. **Result indicator:** Annual financial loss attributable to process safety or process security incidents.

Such dual-purpose indicators provide a balanced view of system performance across safety and security domains and form the basis for resilience monitoring within the RoPSS framework. They link system objectives to measurable performance and ensure they align with governance oversight, operational control, and learning outcomes.

4.3.5. Step 5 – Measure and monitor performance indicators

Experts agreed that indicators are only useful when tracked over time. One industry practitioner (I06) stated, *"Indicators only matter if we monitor them consistently. One-off checks do not tell you whether resilience is improving."* A regulator (G04) explained, *"Trends over time are what convince management. A single data point will never change behavior."* Several experts also noted that limited resources may hinder systematic monitoring, reinforcing the need for pragmatic approaches and progressive implementation.

This step introduces standardized five-point scales and trend analyses to support consistent benchmarking across time, and where relevant, across facilities. For example, a quarterly dashboard comparing safety barrier reliability and security system uptime can highlight shared vulnerabilities. In one organization, trend data showed that maintenance delays affected both safety interlocks and surveillance cameras, prompting a unified improvement program. Systematic monitoring supports adaptive governance and informed decision-making by enabling organizations to track resilience maturity and prioritize improvements.

4.3.6. Step 6 – Resilience-enhancing strategies

Interviewees emphasized that indicators must drive action in order to create value. A consultant (C02) explained, *"The value of indicators is when they trigger actions like updating a procedure, retraining staff, or fixing a weak point. Otherwise, they are just numbers."* An industry expert (I04) agreed, *"Unless results feed back into change, indicators become a reporting exercise. They must link to strategy."*

This step completes the loop by translating performance insights into specific improvement actions, embedding the Ascension capability in practice. Examples include introducing joint emergency drills after identifying low cross-functional preparedness or revising maintenance schedules after incident data reveal shared vulnerabilities in safety and access-control systems. These strategies connect monitoring with improvement, ensuring that performance trends drive learning, prevention, and governance refinement. In this way, the framework embeds resilience into organizational routines and strengthens system performance over time.

Fig. 6 illustrates how the six steps form a continuous management cycle. Each step is explicitly linked to one or more of the four resilience capabilities, ensuring that resilience is operationalized across both process safety and process security functions. Feedback and learning in the Ascension capability drive continuous improvement and complete the resilience loop.

4.4. Performance indicator catalogue

Building on the six-step framework described above, a catalogue of resilience-oriented performance indicators (PIs) was developed to translate system objectives into measurable practices. The catalogue also serves as the operational bridge connecting systemic integration, coupled safety–security dynamics, and governance-level resilience to day-to-day management practice. The indicators are therefore structured not only to measure technical compliance but also to reflect how organizations anticipate, absorb, adapt, and ascend under complex and interdependent risk conditions.

The catalogue is organized across the four resilience capabilities and the eight disruption types identified in this study, with indicators

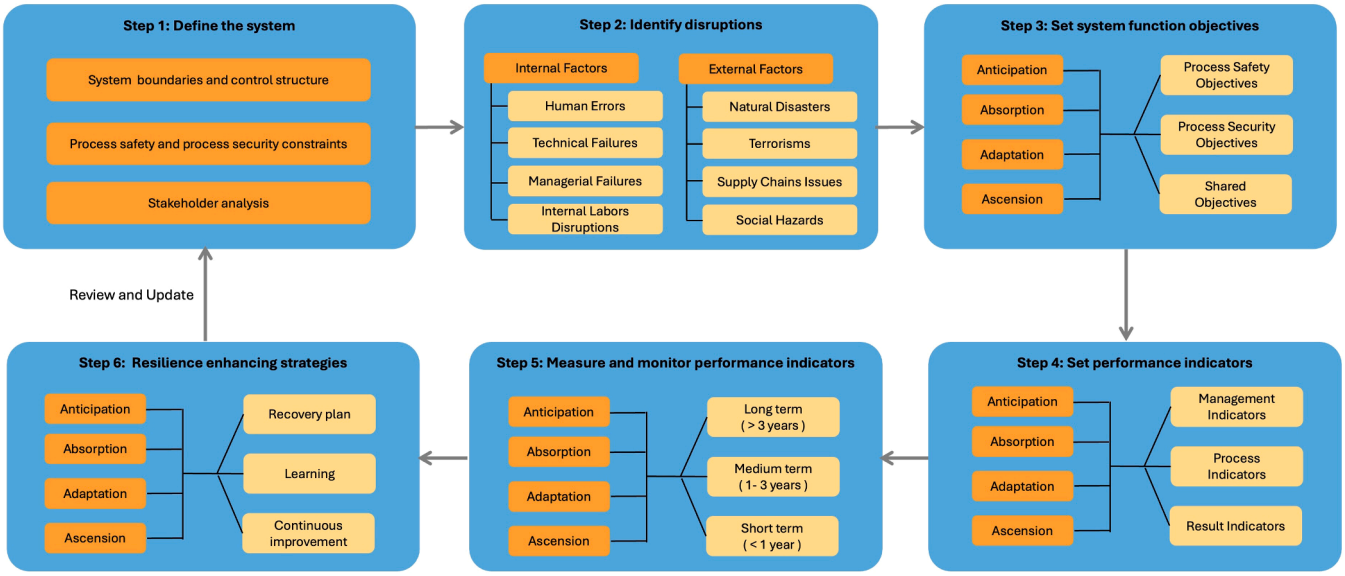

Fig. 6. The six-step RoPSS framework integrates process safety, process security, and the 4As resilience capabilities.

grouped into three functional categories: management, process, and result indicators. Management indicators support systemic anticipation and governance oversight. Process indicators track the performance of coupled systems under both normal and disturbed conditions. Result indicators evaluate recovery, learning, and improvement associated with Ascension. This structure supports balanced coverage of proactive and reactive dimensions and reflects technical, organizational, and cultural contributions to resilience in integrated process safety and process security management.

Experts emphasized that indicator overload must be avoided to maintain usability and managerial focus. One industry expert (I02) commented, *"It's not about collecting hundreds of KPIs. A concise set that covers both safety and security is more practical for us."* A consultant (C02) added, *"When people are overloaded with too many indicators, the important ones get lost. A sharper, integrated set is more useful."* These perspectives reinforce the need for a focused catalogue that prioritizes clarity, dual-purpose coverage, and alignment with the resilience capabilities.

To illustrate the architecture of the indicator catalogue, Table 2 presents a non-exhaustive subset of example indicators showing how management, process, and result measures can be applied across different disruption types and resilience capabilities. These examples highlight the catalogue's breadth while keeping the presentation concise. The complete indicator catalogue with five-point evaluation scales is provided as supplementary materials in associated research repository.

The examples in Table 3 show how indicators function as linking mechanisms between resilience capabilities and operational practice. Management indicators support systemic integration by clarifying resource allocation, leadership commitment, and organizational preparedness across safety and security functions. Process indicators reflect coupled safety-security dynamics by measuring how shared systems perform under both normal and disturbed conditions. Result indicators operationalize governance resilience by capturing the organization's ability to institutionalize lessons, strengthen policies, and support prevention following disruptions, drills, exercises, and simulations. These indicators are therefore intended as an organizational performance measurement architecture, drawing on evidence such as organizational records, maintenance and testing data, training records, incident and near-miss reports, cybersecurity logs, audit findings, and practitioner judgment, rather than as a real-time sensing, automated control, or sensor-fusion model.

4.5. Indicator importance vs. availability matrix

To refine the draft indicator catalogue, a focused expert elicitation was conducted to examine the perceived importance and data availability of the 70 draft indicators. This appraisal combined structured five-point ratings with qualitative feedback from four experts, comprising two from industry and two from government, all with substantial experience in process safety and process security risk management. The exercise was intended as a formative assessment to support indicator refinement and prioritization. For each indicator, mean scores were calculated for both importance and data availability, and these mean values were used to position the indicators within the importance–availability matrix shown in Fig. 7. Indicators with a mean score of 3.0 or above were classified as high on the relevant dimension, while those with a mean score below 3.0 were classified as low.

The matrix was used as a practical screening tool to examine which draft indicators were both conceptually valuable and feasible to operationalize in organizational settings. In this sense, it served not only to highlight potentially useful "quick wins," but also to distinguish indicators that were strategically important yet more difficult to measure from those that were easier to quantify but less informative for resilience-oriented integration. This distinction was particularly relevant in the present study, where the aim was not simply to maximize measurability, but to identify indicators capable of capturing

Table 2
Selected performance indicators by disruption types, resilience capabilities, and indicator categories (illustrative subset of the full catalogue).

Disruption Type	Resilience Capability	Indicator Category	Example Performance Indicator	Dimension
Human Errors	Anticipation	Management	% of operators demonstrating competence in managing safety–security scenarios (via annual assessment)	Safety & Security
Human Errors	Absorption	Process	% of successful safety interlock activations preventing major accidents per year	Safety
Human Errors	Adaptation	Process	% of safety/security procedures revised within 6 months of a relevant incident	Safety & Security
Human Errors	Ascension	Result	Reduction in repeated human-error incidents year-on-year after lessons learned are implemented	Safety
Technical Failures	Anticipation	Management	Ratio of preventive maintenance budget to total budget for critical safety/security equipment for 5 years	Safety & Security
Technical Failures	Absorption	Process	% of equipment with functional secondary containment to mitigate immediate leaks/fires	Safety
Technical Failures	Adaptation	Process	% of critical equipment under real-time condition monitoring, enabling dynamic response	Safety & Security
Technical Failures	Ascension	Result	Reduction in recurrence of technical disruptions following corrective actions (year-on-year)	Safety & Security
Managerial Failures	Anticipation	Management	% of annual budget allocated to non-hardware initiatives (training, risk assessments, investigations)	Safety & Security
Managerial Failures	Absorption	Process	% of emergency decisions executed within predefined timeframes during incidents per year	Safety & Security
Managerial Failures	Adaptation	Process	% of emergency response protocols updated after each incident	Safety & Security

(*continued on next page*)

Table 2 (*continued*)

Disruption Type	Resilience Capability	Indicator Category	Example Performance Indicator	Dimension
			investigation per year	
Managerial Failures	Ascension	Result	Annual rate of injuries from process safety/ security incidents	Safety & Security
Internal Labour	Anticipation	Management	% of workforce receiving risk awareness training for strikes or labor disruptions for the next 2 years	Safety & Security
Internal Labour	Absorption	Process	% of critical processes operable with reduced staffing levels	Safety & Security
Internal Labour	Adaptation	Process	% of scheduled labor relations meetings completed, with > 80% satisfaction among participants for the next 2 years	Safety & Security
Internal Labour	Ascension	Result	% of employees reporting satisfaction with workplace conditions, safety, and security (annual survey)	Safety & Security
Natural Disasters	Anticipation	Management	% of Business Continuity Plan (BCP) procedures reviewed annually for natural disaster risks	Safety & Security
Natural Disasters	Absorption	Process	% of critical equipment supported by backup power systems during blackouts	Safety & Security
Natural Disasters	Adaptation	Process	% of post-disaster assessment findings incorporated into infrastructure upgrades	Safety & Security
Natural Disasters	Ascension	Result	Reduction in downtime from natural disasters (event-to-event or year-on-year)	Safety & Security
Terrorism	Anticipation	Process	% of scheduled vulnerability assessments (physical/cyber) completed (every 3 years)	Security
Terrorism	Absorption	Process	Frequency of security updates/ patches applied to critical control systems (quarterly).	Security
Terrorism	Adaptation	Process	% of security protocols updated after threat assessments or incidents per year	Security
Terrorism	Ascension	Result	Reduction in recurring security breaches/ vulnerabilities after remedial actions	Security
Supply Chain	Anticipation	Management	% of key suppliers undergoing annual reliability/ quality assessments per year	Security
Supply Chain	Absorption	Process	% of critical materials/ components with pre-qualified alternative suppliers per year	Security
Supply Chain	Adaptation	Process	% of corrective actions from supply-route audits implemented on time per year	Security
Supply Chain	Ascension	Result	Reduction in supply chain-related disruptions year-on-year	Security
Social Hazards	Anticipation	Process	% of stakeholder engagement meetings conducted biennially to address social risks, with > 80% satisfaction	Security
Social Hazards	Absorption	Process	Number of contingency measures activated during workforce shortages or utility failures per year	Security
Social Hazards	Adaptation	Process	% of operational procedures updated after major social disruptions per year	Security
Social Hazards	Ascension	Result	Reduction in recurrence of external social hazard disruptions (year-on-year)	Security

meaningful aspects of integrated process safety and process security performance.

Experts generally agreed that some of the most valuable indicators are also among the hardest to measure. For example, one industry expert (I01) commented that *"Competence indicators require observing people performing tasks, not just checking training records. But data are rarely organized that way."* A government expert (G02) added, *"(Data) availability is always the bottleneck. We know what we should measure, but collecting the data is another challenge."* These reflections highlight a pattern common in high-hazard industries: indicators that reflect deeper resilience functions, especially those capturing adaptation, learning, and alignment across safety and security, often require new monitoring processes, enhanced data flows, or cultural change. Conversely, experts cautioned against over-reliance on indicators that are easy to measure

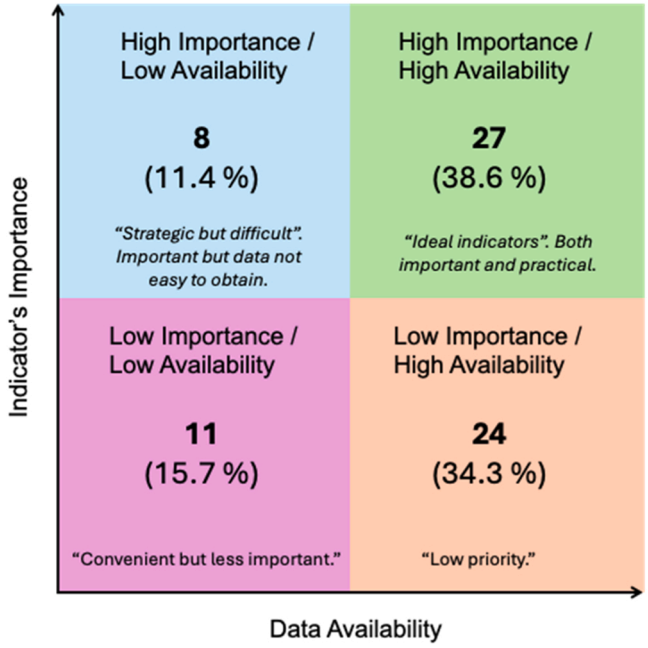

Fig. 7. Importance–Availability Matrix for indicator assessment and practical prioritization.

but offer limited insight into actual resilience performance. One industry expert (I03) observed, *"We have plenty of checklists, but they don't tell us whether the system is truly resilient."* Compliance-based measures, though abundant, rarely capture adaptive capacity or learning quality after disruptions.

Overall, the matrix shows the distribution of the 70 draft indicators across importance and data availability. In this appraisal, 27 indicators (38.6%) were classified as both highly important and readily measurable, representing potential quick wins for early implementation. A further 8 indicators (11.4%) were rated as highly important but less readily measurable, suggesting areas where stronger data systems, clearer evidence sources, or more structured monitoring processes may be needed. By contrast, 24 indicators (34.3%) were considered relatively easy to measure but of lower practical value for resilience-oriented integration, while 11 indicators (15.7%) were rated low on both importance and availability. These patterns were used as a formative input to support refinement and prioritization of the draft catalogue, rather than as a standalone basis for definitive indicator selection.

The refinement decisions informed by this analysis are summarized in Table 3. Indicators were dropped where they were judged to have limited value and weak practical feasibility, merged where substantial conceptual overlap existed, split or reformulated where greater specificity was needed, and reclassified where expert feedback suggested a better fit with another resilience capability. These adjustments improved both the conceptual clarity and the practical usability of the catalogue, while preserving broad coverage across the eight disruption types and four resilience capabilities.

The resulting refined catalogue comprises 50 indicators, distributed across the three indicator types and structured to support field-level application of the RoPSS framework. 10% are management indicators, 80% are process indicators, and 10% are result indicators, distributed across eight disruption types (4–10 per type) and the four resilience capabilities (10–14 per capability). This distribution reflects the operational reality that most resilience-relevant performance occurs at the process level, while also ensuring that governance and learning functions receive explicit attention through management and result indicators. Together, these findings provide a practical basis for integrating performance measurement into organizational practice.

It is important to note that the purpose of this assessment was to guide refinement rather than to produce exhaustive numerical rankings. Detailed indicator-level ratings, along with descriptive statistics, are provided in the associated repository materials. Presenting mean scores for all 70 draft indicators here would add little analytical value, risk overwhelming the central narrative, and is better suited to repository documentation and future case-study implementations. Emphasis is therefore placed on the patterns and practitioner insights that most influenced indicator selection, consolidation, and classification.

Table 3
Refinement of draft performance indicators through importance–availability analysis.

Stage	Number of Indicators	Key Actions	Examples / Notes
Draft catalogue	70	A comprehensive set derived from literature, surveys, and expert interviews.	Broad coverage ensured inclusivity but introduced overlap and feasibility concerns.
Dropped	−10	Indicators judged to have limited value and weak practical feasibility.	E.g., rarely used compliance checks with little added resilience value.
Merged	−14	Overlapping indicators consolidated into broader, more practical measures.	E.g., multiple training coverage metrics combined into one integrated indicator.
Added / Split	+4	A small number of indicators were added or split to capture overlooked aspects or provide clearer measurements.	E.g., separating cyber-incident response drills from physical security drills.
Reclassified	5	Indicators shifted between resilience capabilities based on expert feedback.	E.g., items originally under adaptation moved to Ascension (learning/ improvement).
Refined final catalogue	50	Balanced set covering 4–10 indicators per disruption types across all four resilience capabilities.	Leaner, a more usable set for field implementation.

4.6. Illustrative example of the RoPSS framework

To illustrate how the RoPSS framework may operate in practice, this subsection presents a simplified scenario drawn from typical operations in a mid-sized chlor-alkali plant. The example is illustrative rather than a full case application, as detailed operational scoring and evaluation of the RoPSS indicators are reserved for a subsequent paper within the broader research program.

During routine production, operators observe abnormal pressure fluctuations in the hydrogen compressor, accompanied by intermittent communication failures in the supervisory control and data acquisition (SCADA) interface. Although the deviation initially appears to be a routine technical fault, the simultaneous loss of communication raises concerns about potential cybersecurity interference. This coupled safety–security disturbance provides a practical example of how the six-step framework guides integrated, resilience-oriented decision making.

Step 1 involves defining the system and clarifying responsibilities across safety, security, and operations. In this plant, the hydrogen compressor, associated piping, gas detection systems, emergency shutdown functions, SCADA communication, and networked controllers fall under shared oversight. A rapid joint review involving the process safety engineer, control-room supervisor, and cybersecurity officer establishes a common understanding of the disturbance and helps avoid fragmented troubleshooting. This shared situational awareness provides the basis for coordinated analysis and response.

Step 2 focuses on identifying disruptions by examining potential causes across the eight disruption categories. The team considers

mechanical degradation of the compressor, transmitter failure, control-loop malfunction, maintenance error, misconfigured firewall rules affecting SCADA connectivity, malware, and unauthorized access to the controller. This integrated hazard-threat mapping helps avoid premature assumptions and ensures that accidental and intentional pathways are considered together. This example reflects the systemic and coupled nature of chlor-alkali operations, where hydrogen handling is both safety-critical and security-sensitive.

In **Step 3**, system function objectives are defined to align process safety and process security priorities with the four resilience capabilities. Objectives include verifying the integrity of mechanical and digital safeguards (Anticipation), maintaining containment integrity during the disturbance (Absorption), restoring stable compressor operation and trusted SCADA communication within defined limits (Adaptation), and incorporating lessons from the event into maintenance and cybersecurity practices (Ascension). Establishing these objectives helps the plant navigate trade-offs, such as ensuring that an emergency shutdown does not inadvertently disable critical security logs or delay access needed for timely repair.

Step 4 requires selecting relevant performance indicators from the catalogue. In this example, the selected indicators can be linked to the condition and effectiveness of relevant safety and security controls. Table 4 illustrates how management, process, and result indicators may support monitoring of the coupled hydrogen-compressor and SCADA disturbance. Together, these indicators provide a balanced view of organizational preparedness, control performance, recovery outcomes, and learning.

During **Step 5**, these indicators are measured and monitored to detect early warning patterns and assess whether relevant safety and security controls remain effective. In this example, historical data could show that minor communication faults had increased gradually over several weeks but were not escalated because they fell outside traditional safety metrics. When interpreted together with maintenance records, patching history, abnormal pressure trends, and response-time data, however, these patterns may point to a shared underlying issue affecting both mechanical integrity and digital communication pathways. Identifying such trends allows the plant to take proactive measures rather than relying solely on incident-driven responses. In this way, RoPSS also supports the ALARP principle by helping the organization examine whether existing controls remain maintained, tested, and improved where reasonably practicable.

Finally, **Step 6** converts performance insights into resilience-enhancing strategies. Following a joint after-action review, the plant may upgrade outdated SCADA firmware, revise maintenance routines for compressor components, strengthen dual authorization for critical control-system changes, improve alarm escalation rules, and initiate combined emergency drills involving operators, maintenance staff, the safety team, and security personnel. Lessons from the event are incorporated into updated risk assessment procedures, management-of-change requirements, governance routines, reinforcing Ascension as a capability that extends recovery into structured learning, preventive adaptation, and long-term strengthening of both safety and security systems.

This illustrative example shows how the RoPSS framework supports integrated decision-making when addressing coupled disruptions. By aligning objectives, indicators, control monitoring, ALARP-oriented review, and iterative learning across safety and security, the framework illustrates how resilience may be operationalized as a continuous process for strengthening system performance over time. The example also clarifies that RoPSS does not replace established risk assessment methods, but provides a resilience-oriented management logic through which process safety and process security controls can be monitored, reviewed, and improved.

Table 4
Illustrative performance indicators for the chlor-alkali example.

Indicator type	Illustrative indicators	Link to RoPSS logic
Management indicators	Annual budget for hydrogen-compressor maintenance and SCADA cybersecurity; Personnel competency in cyber-physical anomaly response; Strategic safety-security objectives for hydrogen handling.	Supports preparedness by ensuring financial resources, competent personnel, and strategic direction before a coupled disruption occurs
Process indicators	Percentage of preventive maintenance tasks completed for the hydrogen compressor within schedule; Percentage of gas detectors tested within schedule; Percentage of critical SCADA/security patches implemented within the required timeframe	Monitors whether mechanical, protective, and digital controls remain available, reliable, tested, and maintained during operation
Result indicators	Recurrence of compressor/SCADA disturbances; Corrective-action closure; Lessons incorporated into procedures, drills, training, and governance review	Tracks recurrence, corrective-action completion, and institutional learning after the disturbance

5. Discussion

The results presented in Section 4 show how the ROPSS framework translates resilience engineering principles into a structured, practitioner-informed management cycle. Developed through an iterative synthesis of literature, survey insights, expert interviews, and focused expert elicitation, the framework addresses persistent integration challenges by bringing process safety and process security into a shared, resilience-oriented perspective. This section discusses the theoretical, practical, and methodological implications of the RoPSS framework and positions it within the broader discourse on integrated risk management in the CPI.

5.1. Conceptual and practical contributions

5.1.1. Unifying safety and security within a systemic paradigm

A core contribution of this study is the positioning of process safety and process security as interdependent subsystems within a single socio-technical risk landscape. Traditionally, these domains have evolved through separate regulatory regimes, professional communities, and analytical tools, resulting in parallel management systems. The RoPSS framework suggests that contemporary industrial infrastructures, which are characterized by digitalization, automation, and tightly coupled processes, require a systemic perspective that recognizes shared failure pathways and common risk factors. This integrative view aligns with systems-theoretic perspectives that conceptualize resilience as an emergent property shaped by interactions among technical, human, and organizational components. By embedding safety and security within a unified framework, this study advances the conceptual foundation for managing complex, hybrid disruptions in modern CPI operations.

5.1.2. Coupled-risk trade-offs and co-evolution

This research highlights the inherently coupled nature of safety and security risks. Actions intended to strengthen one dimension may influence the other, producing trade-offs that require deliberate management. Examples surfaced in the expert interviews, such as resolving conflicts between evacuation and lockdown decisions or balancing transparency in safety reporting with confidentiality in security protocols. These tensions are not merely isolated operational dilemmas; they reflect deeper socio-technical interdependencies across infrastructures, human behaviors, and digital systems.

The RoPSS framework contributes by framing these interactions as co-evolving dynamics rather than static trade-offs. Through combined disruption classification and shared objectives across resilience

capabilities, the framework provides a conceptual basis for understanding how control measures, coordination, and technological subsystems interact across safety–security boundaries.

5.1.3. Governance-level resilience and cross-boundary learning

Another conceptual contribution lies in extending resilience beyond operational performance to include governance-level functions. Expert interviews revealed fragmented reporting channels, limited leadership ownership, and weak feedback loops as major barriers to sustained integration. These findings suggest that resilience does not emerge solely from frontline systems but is shaped by higher-level organizational processes that influence resource allocation, accountability, strategic decision-making, and long-term learning.

The framework embeds governance functions within each resilience capability and emphasizes leadership roles, policy alignment, and institutionalized learning. This advances existing literature by linking operational resilience with organizational governance and showing how cross-boundary learning can be formalized across managerial layers.

5.1.4. Ascension as an evolutionary resilience capability

Introducing Ascension is also a central contribution of this study. While anticipation, absorption, and adaptation are widely recognized, many resilience models place less explicit emphasis on how recovery-related learning is consolidated into longer-term organizational improvement. In the RoPSS framework, Ascension is proposed as an evolutionary capability that integrates recovery, learning, continuous improvement, and prevention. In this sense, it does not replace established resilience functions such as Hollnagel's learn cornerstone, but makes more explicit the longer-term trajectory through which operational experience is translated into governance adaptation, preventive redesign, and system strengthening.

Expert insights consistently pointed to weak learning mechanisms and limited cross-functional feedback as impediments to improvement. Formalizing Ascension provides a more complete account of how resilience evolves, linking frontline experience with governance reform and strategic foresight.

5.1.5. Embedding RoPSS within existing process safety management logic

For practical implementation in the CPI, the RoPSS framework should be understood not as a replacement for existing process safety management systems, but as an integrative and continuous-improvement layer that connects process safety and process security through a resilience-oriented management logic. In this sense, RoPSS operates primarily on top of, and alongside, established management arrangements such as OSHA Process Safety Management (PSM), CCPS Risk-Based Process Safety (RBPS), and broader NaTech or Disaster Risk Management (DRM) (Castro Rodriguez et al., 2025; Nwankwo et al., 2020). At the same time, several RoPSS steps, particularly defining the system, identifying disruptions, and setting system function objectives, can also inform upstream planning and risk-identification activities. Table 5 provides an illustrative alignment of the six RoPSS steps with familiar process safety and disaster management logic.

Table 6 shows that the six RoPSS steps are compatible with established process safety and resilience-related practices, while adding a clearer integrative logic for combined process safety and process security management. In particular, RoPSS extends conventional hazard-focused approaches by incorporating intentional disruptions, coupled safety-security interactions, system-function thinking, and a structured indicator architecture linked to the four resilience capabilities. It is therefore best understood as a resilience-oriented framework that complements existing management systems by strengthening cross-domain coordination, performance measurement, and longer-term learning across safety and security functions.

The six-step RoPSS framework also aligns with management logics familiar to practitioners. Several experts noted similarities with the Plan-Do-Check-Act (PDCA) cycle. Although PDCA was not used as a design template, the correspondence is intuitive: Anticipation relates to planning, Absorption to doing, Adaptation to checking and adjusting, and Ascension to acting through learning and improvement. This correspondence may support usability by helping embed resilience-oriented thinking within familiar industrial management processes.

5.2. Methodological reflections and limitations

The methodological design combined literature synthesis, practitioner surveys, expert interviews, and focused expert elicitation, enabling the RoPSS framework to be shaped through both conceptual grounding and practice-informed insights. The semi-structured interviews were particularly valuable for revealing interdependencies and trade-offs between process safety and process security, while the scenario-based elicitation helped experts reason through hybrid and realistic disruptions. The importance-availability assessment added a practical refinement step by identifying indicators that were both meaningful and feasible, thereby supporting the refinement of the final

Table 5
Illustrative alignment of the six RoPSS steps with existing process safety and disaster management logic.

RoPSS step	Related OSHA PSM logic	Related CCPS RBPS logic	Related NaTech /DRM logic	What RoPSS adds
1. Define the system	Process safety information; facility/process boundaries; hazardous chemicals; equipment; procedures	Understanding hazards and risk; process knowledge; stakeholder context	System/context definition; critical infrastructure framing	Defines the plant as a socio-technical safety-security system, including assets, functions, stakeholders, dependencies, and boundaries
2. Identify disruptions	Process hazard analysis; incident scenarios; MOC-related hazards; emergency planning basis	Hazard identification and risk analysis; process safety scenarios	Multi-hazard identification; NaTech interactions; cascading pathways	Expands beyond process hazards to accidental and intentional disruptions, including safety, security, supply chain, labour, natural, and social disruptions
3. Set system function objectives	Safe operating limits; emergency response goals; integrity expectations; operating procedures	Risk-based performance expectations; barrier management; emergency management	Continuity objectives; preparedness and recovery targets	Makes protected system functions explicit: what must continue, what must be restored, and what safety/security objectives must be maintained
4. Set performance indicators	Leading and lagging indicators; audits; training records; maintenance and incident metrics	Metrics; auditing; management review; culture and competency indicators	Vulnerability, preparedness, and recovery indicators	Structures indicators into management, process, and result indicators across resilience capabilities and disruption types
5. Measure and monitor performance indicators	Audits; inspections; incident reporting; performance monitoring; management review	Metrics tracking; audits; management review; learning from experience	Monitoring signals; early warning; vulnerability and recovery tracking	Provides a practical monitoring and scoring process using anchored scales and evidence-based assessment
6. Resilience-enhancing strategies	Corrective actions; MOC; integrity improvement; emergency planning improvement; training; audit follow-up	Risk reduction; barrier strengthening; competency and culture improvement; management review actions	Preparedness, mitigation, recovery, adaptation, and learning measures	Converts measurement results into resilience-enhancing strategies for Anticipation, Absorption, Adaptation, and Ascension

50-indicator catalogue.

Several limitations should be acknowledged. Although the expert sample included participants from industry, government, consultancy, and academia, the number of interviewees was modest, which may limit breadth of representation. As with most qualitative studies, thematic analysis involves interpretive judgment; this was addressed through triangulation across prior literature, survey findings, expert interviews, supervisory discussion, and iterative expert feedback during the refinement of the framework and indicator materials. Furthermore, the framework has not yet undergone full industrial application within this paper. Its use under real operational conditions, as well as the development of plant-level resilience profiling or indexing approaches, requires further empirical study.

Despite these limitations, the methodological approach is consistent with framework-development research in resilience-oriented risk management. The iterative combination of conceptual reasoning, practitioner insight, and focused expert elicitation provides a credible basis for subsequent field application and further empirical evaluation.

6. Conclusion and recommendations

This paper presented the development of the Resilience-oriented Process Safety and Security (RoPSS) framework, an integrated approach that brings process safety and process security within a resilience engineering paradigm. Developed through iterative synthesis of literature, practitioner surveys, expert interviews, and focused expert elicitation, the framework operationalizes resilience through a six-step management cycle supported by a structured performance indicators architecture.

The study contributes to resilience-oriented risk management in four keyways. First, it strengthens the systemic understanding of risk by positioning resilience as an overarching paradigm that connects technical, human, and organizational functions. Second, it clarifies the coupled nature of process safety and process security, illustrating how shared technologies, human factors, and managerial processes create interdependencies that require integrated management. Third, it advances governance-level resilience by demonstrating how leadership structures, accountability mechanisms, and institutional learning shape the conditions under which operational resilience is sustained. Finally, the introduction of Ascension extends resilience beyond restoration by formally incorporating recovery, learning, continuous improvement, and prevention, thereby providing a mechanism that links operational experience to long-term system evolution.

Practically, the framework helps bridge the long-standing divide between safety and security management by offering a coherent structure for defining system boundaries, identifying disruptions, aligning objectives, and monitoring performance across both domains. The resulting indicator catalogue translates resilience into measurable dimensions of managerial capability, operational performance, and learning outcomes. By integrating disruption classification, indicator typology, and a continuous improvement cycle, the framework complements established instruments such as the OECD Guiding Principles, API RP 754, Seveso III Directive, OSHA PSM and CCPS RBPS while extending them to incorporate security and resilience-oriented governance.

Future work should focus on industrial applications and empirical evaluation. As the present paper focuses on framework development and formative expert-informed refinement, RoPSS still requires testing under real operational conditions. Case studies across different chemical facilities will be important for examining usability, assessing indicator feasibility, and refining the framework under real operational conditions. The studies may involve plant-level workshops, baseline indicator scoring, assessment of data availability, calibration of indicator scales, practitioner feedback, and longitudinal monitoring of selected indicators. Such work may also support further development of weighting, aggregation, and plant-level resilience profiling or indexing approaches. In addition, future research may explore how the framework can be linked more closely with digital tools, automated indicator collection, dynamic monitoring, and real-time dashboards, particularly in relation to cyber-physical systems and emerging data infrastructures.

Further research may also examine how interactions of multi-type disruptions can be modeled more explicitly, including cross-impacts between accidental and intentional events, and how the proposed indicator scales may be calibrated against broader empirical evidence. Comparative studies with other established approaches, such as Systems-Theoretic Accident Model and Processes (STAMP), BowTie analysis, and Layer of Protection Analysis (LOPA), may also help clarify the distinct role of RoPSS as a resilience-oriented integrative management framework. Such comparative studies could examine how RoPSS complements barrier-based and systems-theoretic methods by linking risk assessment outputs with resilience capabilities, performance indicators, learning mechanisms, and continuous improvement. In parallel, additional work on systemic risk, coupled with safety-security dynamics, governance mechanisms, and alternative organizational arrangements, will help strengthen the practical embedding of Ascension and support deeper integration across organizational levels. Through continued application, empirical refinement, and comparative learning, the RoPSS framework can evolve from an expert-informed conceptual framework designed for operationalization into a more widely applicable approach for strengthening resilience in the CPI.

CRediT authorship contribution statement

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

Declaration of Competing Interest

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

Acknowledgement

The authors sincerely thank all the professionals and experts who participated in this study. Appreciation is extended to the Public Service Department of Malaysia for awarding the Federal Training Prize scholarship in support of the main author's postgraduate studies.

Data Availability

The interview guide, consent template, integrated codebook, Thematic Analysis Matrices (TAMs) with illustrative quotations, the expert elicitation dataset, and the complete performance indicator catalogue are available through a publicly accessible research repository: https://doi.org/10.4121/cf35f909-c03b-4c9d-bdcd-2254f2bc6d06.

References

Ab Rahim, M.S., Reniers, G., Yang, M., Bajpai, S., 2024. Risk assessment methods for process safety, process security and resilience in the chemical process industry: a thorough literature review. J. Loss Prev. Process. Ind. 88. https://doi.org/10.1016/j.jlp.2024.105274.

Ab Rahim, M.S., Reniers, G., Yang, M., Siwayanan, P., 2025. Integrating process safety and process security risk management: practitioner insights for a resilience-oriented framework. Processes 13 (2). https://doi.org/10.3390/pr13020392.

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

API. (2021). *Process Safety Performance Indicators for the Refining and Petrochemical Industries*.
Aven, T., 2007. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab. Eng. Syst. Saf. 92 (6), 745–754. https://doi.org/10.1016/j.ress.2006.03.008.
Aven, T., 2022. On some foundational issues concerning the relationship between risk and resilience. Risk Anal. 42 (9), 2062–2074. https://doi.org/10.1111/risa.13848.
Ayyub, B.M., 2014. Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. Risk Anal. 34 (2), 340–355. https://doi.org/10.1111/risa.12093.
Bischoff, H.-J., Sinay, J., Vargová, S., 2015. Integrated Risk Management in Industries from the Standpoint of Safety and Security. Trans. V. ŠB Tech. Univ. Ostrav. Saf. Eng. Ser. 9 (2), 1–7. https://doi.org/10.2478/tvsbses-2014-0005.
Blokland, P., Reniers, G., 2020. The Concepts of Risk, Safety, and Security: A Fundamental Exploration and Understanding of Similarities and Differences. In: Bieder Corinne, K., Pettersen Gould (Eds.), The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice. Springer International Publishing, pp. 9–16. https://doi.org/10.1007/978-3-030-47229-0_2.
Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101. https://doi.org/10.1191/1478088706qp063oa.
Casson Moreno, V., Reniers, G., Salzano, E., Cozzani, V., 2018. Analysis of physical and cyber security-related events in the chemical and process industry. Process. Saf. Environ. Prot. 116, 621–631. https://doi.org/10.1016/j.psep.2018.03.026.
Castro Rodriguez, D.J., Barresi, A.A., Demichela, M., 2025. Resilience-based framework for enhancing NaTech risk management in industrial critical infrastructures. Environ. Syst. Decis. 45 (4). https://doi.org/10.1007/s10669-025-10056-9.
CCPS. (2007). *Guidelines for Risk Based Process Safety* (Center for Chemical Process Safety, Ed.). Wiley.
CCPS. (2022). *Managing Cybersecurity in the Process Industries: A Risk-based Approach* (First edition). Wiley and Sons, Inc.
Creswell. (2018). *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches* (Fifth Edition). SAGE.
European Union. (2012). 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). In *Official Journal of the* European Union (L 197; pp. 1–37). ⟨https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0018⟩.
Geng, S., Yang, M., Mitici, M., Liu, S., 2023. A resilience assessment framework for complex engineered systems using graphical evaluation and review technique (GERT). Reliab. Eng. Syst. Saf. 236. https://doi.org/10.1016/j.ress.2023.109298.
Glesner, C., Geysmans, R., Turcanu, C., 2022. Two sides of the same coin? Exploring the relation between safety and security in high-risk organizations. J. Saf. Res. 82, 184–193. https://doi.org/10.1016/j.jsr.2022.05.010.
Hansen, S.T., Antonsen, S., 2024. Taking connectedness seriously. A research agenda for holistic safety and security risk governance. Saf. Sci. 173. https://doi.org/10.1016/j.ssci.2024.106436.
Hollnagel, E., 2006. Resilience – the Challenge of the Unstable. In: Hollnagel, E., David., D.Woods, Leveson, N. (Eds.), Resilience Engineering: Concepts and Precepts (1st Edition. CRC Press, pp. 9–17. https://doi.org/10.1201/9781315605685.
Hosseini, S., Barker, K., Ramirez-Marquez, J.E., 2016. A review of definitions and measures of system resilience. Reliab. Eng. Syst. Saf. 145. https://doi.org/10.1016/j.ress.2015.08.006.
Magnusson, E., Marecek, J., 2015. Doing Interview-based Qualitative Research - A Learner's Guide. Cambridge University Press. https://doi.org/10.1017/CBO9781107449893.
HSE UK. (2006). *Developing process safety indicators: a step-by-step guide for chemical and major hazard industries*. Health and Safety Executive.
Huang, Y., Chen, G., Zhao, Y., Xu, Q., 2025. An advanced dynamic risk assessment method for chemical industry park cyber-physical system based on improved GraphSAGE. Process. Saf. Environ. Prot. 204. https://doi.org/10.1016/j.psep.2025.107990.
Iaiani, M., Casson Moreno, V., Reniers, G., Tugnoli, A., Cozzani, V., 2021. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab. Eng. Syst. Saf. 212. https://doi.org/10.1016/j.ress.2021.107593.
Jain, P., Rogers, W.J., Pasman, H.J., Keim, K.K., Mannan, M.S., 2018. A Resilience-based integrated process systems hazard analysis (RIPSHA) approach: part i plant system layer. Process. Saf. Environ. Prot. 116, 92–105. https://doi.org/10.1016/j.psep.2018.01.016.
Jain, P., Pasman, H.J., Sam Mannan, M., 2020. Process system resilience: from risk management to business continuity and sustainability. Int. J. Bus. Contin. Risk Manag. 10 (1), 47–66. https://doi.org/10.1504/IJBCRM.2020.105615.
Jovanović, A., Øien, K., Choudhary, A., 2018. An indicator-based approach to assessing resilience of smart critical infrastructures. Urban Book Series. Springer, pp. 285–311. https://doi.org/10.1007/978-3-319-68606-6_17.
Kenneth, C.B., Gould, P., 2020. The coupling of safety and security - exploring interrelations in theory and practice. Springer. ⟨http://www.springer.com/series/15119⟩.
Khan, F., Abunada, H., John, D., Benmosbah, T., 2010. Development of risk-based process safety indicators. Process. Saf. Progress. 29 (2), 133–143. https://doi.org/10.1002/prs.10354.
Landucci, G., Khakzad, N., Reniers, G., 2020. Physical security risk assessment tools and applications. Physical Security in the Process Industry. Elsevier, pp. 71–123. https://doi.org/10.1016/b978-0-444-64054-3.00004-4.
Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34. https://doi.org/10.1016/j.ress.2014.10.008.
Leveson, N., 2020. Safety and Security Are Two Sides of the Same Coin. SpringerBriefs in Applied Sciences and Technology. Springer Science and Business Media Deutschland GmbH, pp. 17–27. https://doi.org/10.1007/978-3-030-47229-0_3.
Linkov, T., 2019. Resilience as function of space and time. The Science and Practice of Resilience. Springer, pp. 9–23. https://doi.org/10.1007/978-3-030-04565-4.
Mentges, A., Halekotte, L., Schneider, M., Demmer, T., Lichte, D., 2023. A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. Int. J. Disaster Risk Reduct. 96. https://doi.org/10.1016/j.ijdrr.2023.103893.
Meyer, T., Reniers, G., 2022. Risk management principles. Engineering Risk Management, Thrd Edition. De Gruyter, pp. 43–109.
Nwankwo, C.D., Theophilus, S.C., Arewa, A.O., 2020. A comparative analysis of process safety management (PSM) systems in the process industry. J. Loss Prev. Process. Ind. 66. https://doi.org/10.1016/j.jlp.2020.104171.
OECD. (2008a). *Guidance on Developing Safety Performance Indicators for Industry*. OECD.
OECD. (2008b). *Guidance on Developing Safety Performance Indicators for Public Authorities and Communities/ Public*. OECD.
OECD. (2019). *OECD Reviews of Risk Management Policies - Good Governance for Critical Infrastructure Resilience* (OECD Reviews of Risk Management Policies). OECD Publishing. https://doi.org/10.1787/02f0e5a0-en.
OECD. (2023). *OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response - Third Edition* (Series on Chemical Accidents). OECD. https://doi.org/10.1787/162756bf-en.
Pasman, H., Rogers, W., 2014. How can we use the information provided by process safety performance indicators? Possibilities and limitations. J. LOSS Prev. Process Industries 30, 197–206. https://doi.org/10.1016/j.jlp.2013.06.001.
Pasman, H., Kottawar, K., Jain, P., 2020. Resilience of process plant: What, why, and how resilience can improve safety and sustainability. Sustain. (Switz.) 12 (15). https://doi.org/10.3390/su12156152.
Patriarca, R., Bergström, J., Di Gravio, G., Costantino, F., 2018. Resilience Engineering: Current Status of the Research and Future Challenges. In: Safety Science, 102. Elsevier B.V, pp. 79–100. https://doi.org/10.1016/j.ssci.2017.10.005.
Pawar, B., Park, S., Hu, P., Wang, Q., 2021. Applications of resilience engineering principles in different fields with a focus on industrial systems: a literature review. J. Loss Prev. Process. Ind. 69. https://doi.org/10.1016/j.jlp.2020.104366.
Perrow, C., 1999. Normal Accidents: Living with High Risk Technologies - Updated Edition. Princeton University Press.
Pettersen, K.A., Bjørnskau, T., 2015. Organizational contradictions between safety and security - Perceived challenges and ways of integrating critical infrastructure protection in civil aviation. Saf. Sci. 71 (PB), 167–177. https://doi.org/10.1016/j.ssci.2014.04.018.
Pettersen Gould, K., Bieder, C., 2020. Safety and security: the challenges of bringing them together. SpringerBriefs in Applied Sciences and Technology. Springer Science and Business Media Deutschland GmbH, pp. 1–8. https://doi.org/10.1007/978-3-030-47229-0_1.
Process Safety Management of Highly Hazardous Chemicals Standard (29 CFR 1910.119), Pub. L. 29 CFR 1910.119, U.S. Department of Labor (1992). ⟨https://www.osha.gov/process-safety-management⟩.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27 (3), 183–213.
Reniers, G., Cremer, K., Buytaert, J., 2011. 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. 19 (11), 1239–1249. https://doi.org/10.1016/j.jclepro.2011.03.002.
Reniers, G., Landucci, G., Khakzad, N., 2020. What safety models and principles can be adapted and used in security science? J. Loss Prev. Process. Ind. 64. https://doi.org/10.1016/j.jlp.2020.104068.
Schoemaker, P.J.H., 1993. Multiple scenario development: its conceptual and behavioral foundation. Manag. J. 14 (3). https://doi.org/10.1002/smj.4250140304.
Schulman, P.R., 2020. Safety and Security: Managerial Tensions and Synergies. In: Bieder Corinne, K., Pettersen Gould (Eds.), The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice. Springer International Publishing, pp. 87–95. https://doi.org/10.1007/978-3-030-47229-0_9.
Sultana, S., Andersen, B.S., Haugen, S., 2019. Identifying safety indicators for safety performance measurement using a system engineering approach. Process. Saf. Environ. Prot. 128, 107–120. https://doi.org/10.1016/j.psep.2019.05.047.
Sun, H., Qi, M., Yang, M., Wang, F., Wang, H., 2025. Multiparametric resilience assessment of chemical process systems incorporating process dynamics and independent protection layers. Process. Saf. Environ. Prot. 197. https://doi.org/10.1016/j.psep.2025.107018.
Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., Blokland, P., 2016. Process safety indicators, a review of literature. J. Loss Prev. Process. Ind. 40. https://doi.org/10.1016/j.jlp.2015.12.020.
Tong, Q., Yang, M., Zinetullina, A., 2020. A dynamic bayesian network-based approach to resilience assessment of engineered systems. J. Loss Prev. Process. Ind. 65. https://doi.org/10.1016/j.jlp.2020.104152.
Vert, M., Sharpanskykh, A., Curran, R., 2021. Adaptive resilience of complex safety-critical sociotechnical systems: toward a unified conceptual framework and its formalization. Sustain. (Switz.) 13 (24). https://doi.org/10.3390/su132413915.
Woods, D.D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9. https://doi.org/10.1016/j.ress.2015.03.018.
Yang, M., Sun, H., Geng, S., 2023. On the quantitative resilience assessment of complex engineered systems. Process. Saf. Environ. Prot. 174, 941–950. https://doi.org/10.1016/J.PSEP.2023.05.019.

Yarveisy, R., Gao, C., Khan, F., 2020. A simple yet robust resilience assessment metrics. Reliab. Eng. Syst. Saf. 197, 106810. https://doi.org/10.1016/J.RESS.2020.106810.
Yarveisy, R., Sun, H., Yang, M., Pasman, H., 2022. Resilience Analysis of Digitalized Process Systems, 6. Elsevier, pp. 591–629. https://doi.org/10.1016/bs.mcps.2022.05.002.
Ylönen, M., Tugnoli, A., Oliva, G., Heikkilä, J., Nissilä, M., Iaiani, M., Cozzani, V., Setola, R., Assenza, G., van der Beek, D., Steijn, W., Gotcheva, N., Del Prete, E., 2022. Integrated management of safety and security in Seveso sites - sociotechnical perspectives. Saf. Sci. 151. https://doi.org/10.1016/j.ssci.2022.105741.
Yuan, S., Yang, M., Reniers, G., 2024. Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants. Comput. Ind. 155. https://doi.org/10.1016/j.compind.2023.104056.
Yuan, S., Reniers, G., Yang, M., 2025. Dynamic and integrated safety and security barrier management: a new framework to manage major event risks in chemical plants. J. Loss Prev. Process. Ind. 96. https://doi.org/10.1016/j.jlp.2025.105632.
Zeng, T., Wei, L., Duo, Y., Yang, G., Chen, S., 2025. Resilience-based design of barrier system to mitigate fire-driven escalation in process plants. Process. Saf. Environ. Prot. 199. https://doi.org/10.1016/j.psep.2025.107319.
Zhang, F., Yang, J., Li, J., Zhang, J., Li, J., Chen, L., Diao, X., Wang, Q., Dou, Z., 2024. Integrated physical safety–cyber security risk assessment based on layers of protection analysis. Chem. Eng. Res. Des. 212, 405–420. https://doi.org/10.1016/j.cherd.2024.10.036.
Zinetullina, A., Yang, M., Khakzad, N., Golman, B., Li, X., 2021. Quantitative resilience assessment of chemical process systems using functional resonance analysis method and Dynamic Bayesian network. Reliab. Eng. Syst. Saf. 205. https://doi.org/10.1016/j.ress.2020.107232.
Zio, E., 2018. The future of risk assessment. Reliab. Eng. Syst. Saf. 177, 176–190. https://doi.org/10.1016/j.ress.2018.04.020.