TU Delft

Delft University of Technology

Document Version
Final published version

Citation (APA)
Bin Ab Rahim, M. S. (2026). *Integrating Process Safety and Process Security Risk Management through a Resilience-oriented Framework*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:9ef4fa25-8bed-4e27-8d49-398b518627c6

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

Copyright
In case the licence states “Dutch Copyright Act (Article 25fa)”, this publication was made available Green Open Access via the TU Delft Institutional Repository pursuant to Dutch Copyright Act (Article 25fa, the Taverne amendment). This provision does not affect copyright ownership.
Unless copyright is transferred by contract or statute, it remains with the copyright holder.

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

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

This work is downloaded from Delft University of Technology.

Integrating Process Safety and Process Security Risk Management

through a Resilience-oriented Framework



Muhammad Shah Bin Ab Rahim



Integrating Process Safety and Process Security Risk Management through a Resilience-oriented Framework

Muhammad Shah Bin Ab Rahim

The research is supported by the Public Service Department of Malaysia under the Federal Training Prize 2022 with reference number JPA(1)830227015745.

Keywords: resilience engineering; process safety; process security; integrated risk management; performance indicators; chemical process industry; coupled safety-security risk

Printed by: Ridderprint | www.ridderprint.nl
Cover & layout design: Anastasia Gangaev | www.ridderprint.nl
Copyright: 2026 by M.S. Bin Ab Rahim
ISBN: 978-94-6537-656-1

An electronic version of this dissertation is available at: http://repository.tudelft.nl

Integrating Process Safety and Process Security Risk Management through a Resilience-oriented Framework

Dissertation

for the purpose of obtaining the degree of doctor

at Delft University of Technology

by the authority of the Rector Magnificus,

Prof.dr.ir. H. Bijl,

chair of the Board for Doctorates

to be defended publicly on

Wednesday, 2 September 2026 at 10:00

by

Muhammad Shah BIN AB RAHIM

This dissertation has been approved by the promotors.

Composition of the doctoral committee:

Rector Magnificus	*chairperson*
Prof.dr.ir. G.L.L.M.E. Reniers	Delft University of Technology, *promotor*
Dr. M. Yang	Delft University of Technology, *promotor*
Em.prof.dr. A. Mohd Shariff	Universiti Teknologi PETRONAS, Malaysia, *external adviser*

Independent members:

Prof.dr. S. Bajpai	National Institute of Technology Jalandhar, India
Prof.mr.dr. J.A. de Bruijn	Delft University of Technology
Dr. A. Buang	Universiti Teknologi PETRONAS, Malaysia
Prof.dr.ing. B. Fabiano	University of Genoa, Italy
Prof.dr.ir. P.H.A.J.M. van Gelder	Delft University of Technology

“ The past resembles the future more than one drop of water resembles another. “

— Ibn Khaldun, The Muqaddimah (1377)

TABLE OF CONTENTS

Summary X
Samenvatting XVIII

Chapter 1 Introduction 1
1.1 Background 3
1.1.1 Chemical process industry, process safety, and process security 3
1.1.2 Resilience engineering 8
1.2 Problem statement 10
1.3 Research aim and objectives 11
1.4 Research questions 11
1.5 Research design 14
1.6 Contributions 18
1.7 Dissertation outline 19

Chapter 2 Mapping the Integration Gap: Methods for Process Safety, Process Security, and Resilience in the Chemical Process Industry 21
2.1 Introduction 24
2.1.1 Context 24
2.1.2 Need for this review 27
2.1.3 Aim and scope of the review 29
2.2 Methodology 30
2.2.1 The review protocol 30
2.2.2 Formulation of the research question 30
2.2.3 Systematic searching strategies 30
2.2.4 Screening 31
2.2.5 Eligibility 33
2.2.6 Data extraction and analysis 34
2.3 Results 34
2.3.1 Current trend of publications related to process safety, security, and resilience assessment in the CPI 34
2.3.2 Overview of process safety risk assessment, process security risk assessment, and process resilience assessment methods 37
2.3.3 Type of approach, tools, and stage of assessment 45
2.4 Discussion 49
2.4.1 Strengths and limitations of process safety, security, and

resilience assessment methods 49
2.4.2 Future Research 56
2.5 Conclusion and recommendations 57

Chapter 3 Practitioner Perspectives on Integration: Process Safety, Process Security, and Resilience Engineering in Practice 59
3.1 Introduction 62
3.2 Methodology 65
3.3 Results 67
3.3.1 Respondent demographics 67
3.3.2 Perception on integration usefulness 70
3.3.3 Awareness and perception of the resilience concept 72
3.3.4 Importance of different societal values 78
3.3.5 Barriers and enablers for integration 83
3.3.6 Proposed strategies for integrating process safety and process security 86
3.4 Discussions 90
3.4.1 Interpretation of findings 90
3.4.2 Synthesis of the grand themes 95
3.4.3 Recommendations 97
3.5 Conclusions 99

Chapter 4 Developing the RoPSS Framework: A Resilience-oriented Approach to Integrated Process Safety and Process Security Risk Management 101
4.1 Introduction 104
4.2 Conceptual and theoretical construct 107
4.2.1 Resilience as a systemic risk management paradigm 107
4.2.2 Coupled process safety–security dynamics in socio-technical systems 109
4.2.3 Resilience capabilities and the evolutionary role of Ascension 111
4.2.4 From operational to governance resilience 114
4.2.5 Resilience measurement and performance indicators 116
4.2.6 Conceptual integration towards a resilience-oriented framework 119
4.3 Methodology 121
4.3.1 Research design and rationale 121
4.3.2 Expert interviews with scenario-based elicitation 122
4.3.3 Data analysis and coding 125
4.3.4 Assessing indicator importance and availability 126
4.3.5 Trustworthiness and ethical considerations 127
4.4 Results 127

4.4.1 Challenges and integration requirements 127
4.4.2 Resilience capabilities reflected in expert insights 130
4.4.3 The Resilience-oriented Process Safety and Security (RoPSS) framework 132
4.4.4 Performance indicator catalogue 138
4.4.5 Indicator importance vs. availability matrix 142
4.4.6 Illustrative example of the RoPSS framework 146
4.5 Discussion 148
4.5.1 Conceptual and practical contributions 149
4.5.2 Methodological reflections and limitations 153
4.6. Conclusion and recommendations 154

Chapter 5 Operationalizing the RoPSS Framework: Application and Baseline Resilience Profiling in Chemical Plant Settings 157
5.1 Introduction 160
5.1.1 From conceptual integration to operational use 160
5.1.2 Research objective and guiding questions 161
5.1.3 Scope and boundaries of the study 162
5.2. Framework overview and implementation context 163
5.2.1 Overview of the RoPSS framework 163
5.2.2 Case study selection and context 166
5.2.3 Scope of framework application 168
5.3. Methodology 170
5.3.1 Research design 170
5.3.2 Data sources 172
5.3.3 RoPSS operationalization procedure 173
5.3.4 Indicator scoring protocol, missing data handling, and aggregation 173
5.3.5 Context mapping variables 175
5.3.6 Researcher role and confidentiality 176
5.4. Results 176
5.4.1 Operationalization of the RoPSS framework 176
5.4.2 Baseline resilience profiles 177
5.4.3 Cross-case contrasts 187
5.4.4 Resilience-enhancing strategies 189
5.5. Discussion 192
5.5.1 How RoPSS supports integrated process safety–security management in practice 192
5.5.2 RoPSS as a mixed-method diagnostic and sense-making tool 194
5.5.3 Limitations and implications for use 197

5.6. Conclusion 198

Chapter 6 Conclusion and Recommendations 199
6.1 Key findings in relation to the research questions 201
6.1.1 The resilience-oriented approach 201
6.1.2 The fragmented methods 202
6.1.3 The practitioner insights 203
6.1.4 The integrated framework 203
6.1.5 The operationalization 204
6.1.6 The overall synthesis 205
6.2 Contributions of the thesis 207
6.2.1 Theoretical contributions 207
6.2.2 Practical contributions 209
6.3 Methodological reflections and limitations 211
6.4 Recommendations 214
6.4.1 Recommendations for practice and policy 215
6.4.2 Recommendations for future research 218
6.5 Final conclusion 220

Appendix 221
References 223
Appendix A: Analysis of type, techniques, and stage of assessment 241
Appendix B: Balancing societal values 249
Appendix C: Full catalogue of resilience-oriented performance indicators 251
Appendix D: Context mapping headings and example observations 271
Appendix E: Operationalization artifacts and outputs 273
Appendix F: Online research dataset 275
Acknowledgements 276
Curriculum Vitae 280
List of Publications 282

SUMMARY

"I have studied all people in their actions, and I have found that all of them, without exception, seek to attain only one goal: to rid themselves of anxiety."

— Ibn Hazm (994–1064)

This thesis responds, in part, to that enduring human concern. Ibn Hazm's reflection speaks to a fundamental desire for safety, security, stability, freedom from harm, and, indirectly, for resilience. In the chemical process industry (CPI), such anxiety may be understood not only as a personal feeling, but also as a reflection of uncertainty, vulnerability, and the possibility of harm arising from accidents, malicious acts, and operational disruptions. Process safety and process security are both concerned with reducing these threats, yet in practice they are often managed separately. This thesis therefore explores how these domains can be brought together through a resilience-oriented approach, with the aim of helping chemical plants not only prevent and withstand disruptions, but also adapt, recover, and grow stronger from them.

The CPI contributes significantly to economic development, but it is also characterized by hazardous substances, complex technologies, tightly coupled operations, and the potential for major-hazard events. Within this context, this thesis focuses on major-hazard, or "Type II," risks: relatively rare but potentially catastrophic events such as major fires, explosions, toxic releases, sabotage, terrorism, and cyber-physical disruptions. Although process safety and process security both seek to protect people, assets, operations, and the environment from such events, they have historically developed as separate domains, shaped by different regulatory traditions, analytical approaches, and professional cultures. This separation can create duplication, unresolved trade-offs, and blind spots in the management of major-hazard risks.

Against this background, the main research question of this thesis is: **How can process safety and process security risk management be integrated through a resilience-oriented framework for the chemical**

process industry? To address this question, the thesis is guided by four sub-research questions concerning:

1. What does the existing literature reveal about methods for process safety, process security, and resilience in the chemical process industry, and their implications for integrated risk management?
2. How do practitioners perceive the integration of process safety and process security risk management through a resilience engineering lens?
3. How can a resilience engineering paradigm be translated into an integrated risk management approach for process safety and process security in the chemical process industry?
4. How can a resilience-oriented framework be operationalized and applied in chemical plant settings?

The overall aim of the thesis is therefore to develop and operationalize a resilience-oriented framework for integrated process safety and process security risk management in the CPI. To achieve this, the thesis adopts a multi-method research design with a sequential and cumulative logic. It begins by establishing the state of knowledge through a systematic literature review, then incorporates practitioner perspectives through a mixed-methods survey, proceeds to framework development through conceptual synthesis, expert interviews, and elicitation, and finally operationalizes the framework in two chemical plant case studies. This design enables the thesis to move from problem diagnosis to conceptual development and practical application, while ensuring that the proposed framework is informed by both theory and practice.

The thesis first examines the fragmented state of existing knowledge on process safety, process security, and resilience. The systematic literature review shows that the field is methodologically rich but conceptually fragmented. Process safety methods are comparatively mature and supported by a wide range of established tools, whereas process security assessment and resilience assessment remain less consolidated. Although some methods show promise for addressing uncertainty, interdependencies, and socio-technical complexity, most studies still treat process safety, process security, and resilience as separate or only partially connected domains. This confirms that the integration gap is not merely assumed, but is clearly visible in the existing literature.

The thesis then investigates practitioner perspectives on integration through a resilience lens. The survey findings show that practitioners

generally regard the integration of process safety and process security as useful and beneficial. Most respondents considered such integration worthwhile, particularly because it may reduce redundancy, improve the use of resources, and strengthen the comprehensiveness of risk management. At the same time, practitioner support was found to be conditional rather than uncomplicated. Important barriers include limited knowledge and awareness, insufficient resources, siloed communication, and weak coordination between safety and security functions. In addition, although resilience-oriented thinking was generally viewed positively, familiarity with resilience concepts remained mostly slight to moderate. These findings suggest that resilience can serve as a promising lens for integration, but only if it is translated into practical language, routines, and tools that practitioners can recognize and apply. The survey also highlighted that integration is not only technical, but also involves trade-offs between values and priorities that may shift across scenarios.

Next, the thesis develops its core conceptual contribution: the Resilience-oriented Process Safety and Process Security (RoPSS) framework. Drawing on resilience engineering, expert interviews, and expert elicitation, the thesis proposes that process safety and process security should be understood not as parallel domains, but as coupled socio-technical subsystems within a shared major-hazard landscape. To structure this integration, the RoPSS framework is organized around four resilience capabilities: Anticipation, Absorption, Adaptation, and Ascension. These capabilities are embedded within a six-step management cycle and linked to eight disruption categories and three performance indicator types. In this way, the framework translates resilience engineering from an abstract perspective into a structured integrated risk management approach for the CPI.

A particularly important contribution of the thesis is the introduction of Ascension as a distinct resilience capability. While many resilience formulations stop at restoration, response, or learning, this thesis argues that integrated risk management in the CPI also requires a longer-term capability that captures recovery, institutional learning, continuous improvement, prevention, and stronger governance. Ascension is proposed to reflect this broader and more forward-looking dimension. In doing so, it extends resilience thinking beyond immediate restoration and emphasizes how lessons and recovery experience can be translated into stronger

future performance. This is especially relevant for complex chemical process systems in which accidental and intentional disruptions interact with technical arrangements, organizational routines, and governance structures over time.

The thesis then focuses on operationalization and practical application. The RoPSS framework is translated into a structured semi-quantitative instrument and applied in two chemical plant case studies, one in Malaysia and one in the Netherlands. These applications demonstrate that the framework can function not only as a conceptual model, but also as a practical diagnostic and sense-making tool. Using the same disruption-organized structure, the case studies generated baseline resilience profiles, disruption-by-capability heatmaps, indicator-type summaries, and qualitative resilience-enhancing strategies. Although the two plants differed in context, governance arrangements, evidence availability, and access conditions, both applications produced auditable baseline profiles. This suggests that the framework is sufficiently flexible to support structured use under realistic industrial conditions.

An important practical finding concerns the treatment of indicators that could not be scored. In the case studies, some items were marked as “N/A” because they fell outside plant-level ownership, were not applicable within the local context, or could not be evidenced within the available timeframe. Rather than treating these as simple missing data, the thesis interprets them as meaningful operationalization outcomes that reveal assessment boundaries and governance conditions. This helps distinguish between genuine capability gaps and limitations arising from scope, responsibility, or evidence access. As such, the operationalization stage reinforces the importance of boundary awareness, evidence traceability, and context sensitivity in resilience-oriented and integrated assessment.

Collectively, the findings of the thesis show a coherent progression. The literature review establishes that process safety, process security, and resilience remain fragmented in the existing body of knowledge. The practitioner survey demonstrates that integration is desired, but also challenged in practice. The framework-development study responds to this need by translating resilience engineering into the RoPSS framework. Finally, the case studies show that the framework can be operationalized in real plant settings to generate useful diagnostic outputs and improvement

directions. Overall, the thesis concludes that a more integrated approach to process safety and process security in the CPI is both well justified and practically feasible, provided that it is supported by a resilience-oriented perspective that recognizes the socio-technical and governance nature of major-hazard systems.

This thesis makes several theoretical contributions. It advances the understanding of process safety and process security as interdependent socio-technical subsystems within a shared risk landscape. It further demonstrates how resilience can serve as an organizing paradigm for integrated risk management in the CPI, rather than remaining an abstract concept. The thesis also refines resilience theory by introducing Ascension as a distinct capability and by linking operational resilience with governance resilience in a single framework. In addition, it offers a structured conceptual architecture that connects disruption categories, resilience capabilities, and performance indicator types, thereby providing a more systematic basis for integrated risk management.

The thesis also makes several practical contributions. It provides the RoPSS framework as a structured management approach for integrating process safety and process security. It offers an indicator-based assessment system that can support baseline profiling, monitoring, and reflection. It shows that the framework can be applied across different industrial conditions and can generate outputs that help organizations identify strengths, weak points, and priorities for improvement. It also highlights the importance of ownership boundaries, evidence traceability, and follow-up strategies in real-world resilience assessment. Beyond plant-level use, the findings are also relevant to regulators, inspectors, policymakers, and industrial-complex coordinators seeking more integrated and resilience-oriented approaches to major-hazard governance.

At the same time, the thesis acknowledges several limitations. The literature review was bounded by specific inclusion criteria and may not have captured all relevant emerging work. The practitioner survey was exploratory and based on a relatively small, non-random sample, concentrated mainly in Malaysia and the Netherlands. The framework development stage should be interpreted as expert-informed and formative rather than as conclusive validation. Likewise, the case studies demonstrate practical operationalization and use, but do not establish

predictive validity, broad generalizability, or effectiveness outcomes over time. The indicator system also remains developmental in some respects, particularly regarding qualitative judgement, inter-rater consistency, evidence availability, and aggregation choices. These limitations do not undermine the value of the thesis, but rather indicate the developmental stage of the framework and the directions for further research.

The findings of the thesis also point to several implications for practice and future research. For practice, the thesis suggests that chemical plants should move beyond separate safety and security routines and establish stronger mechanisms for joint governance, coordination, disruption mapping, and integrated objectives. Organizations should incorporate resilience-oriented thinking more explicitly into management systems and make greater use of integrated indicators, while remaining attentive to evidence boundaries and ownership issues. Greater investment is also needed in competence development, cross-training, communication, and longer-term learning beyond immediate recovery. At the policy level, the thesis suggests that regulators and governance actors should encourage stronger alignment between process safety and process security arrangements, particularly in emerging cross-domain areas such as cyber-physical threats and industrial-cluster governance.

For future research, the thesis recommends broader application of the RoPSS framework across different CPI contexts, longitudinal studies of resilience profiles over time, continued refinement of the indicator system, exploration of digital decision-support tools, and closer examination of cyber-physical and cross-boundary settings. It also calls for comparative studies between RoPSS and established approaches such as STAMP, FRAM, and Bowtie analysis, in order to clarify where RoPSS offers additional value, where it complements existing methods, and how its resilience-oriented and integration-focused features compare with more established approaches for managing coupled safety-security risks. Finally, the thesis calls for further study of the framework's effectiveness, including whether its use leads to improved decisions, stronger resilience performance, and better integration outcomes in practice. Such work would represent an important next step in the maturation of RoPSS as both a conceptual and practical contribution to the field.

In conclusion, this thesis addresses the longstanding fragmentation between process safety and process security risk management in the chemical process industry. It shows that this separation limits the ability of organizations to understand and manage accidental and intentional disruptions in an integrated way. In response, the thesis develops and operationalizes the RoPSS framework, which integrates both domains through the four resilience capabilities of Anticipation, Absorption, Adaptation, and Ascension within a six-step management cycle. Through its conceptual development, indicator architecture, and application in two chemical plant case studies, the thesis demonstrates that a resilience-oriented approach can provide both a meaningful conceptual basis and a practical pathway for more integrated risk management of Type II risks in the CPI. Overall, the thesis concludes that a more integrated approach to process safety and process security in the CPI is both well justified and practically feasible. Ultimately, the value of a resilience-oriented integration of process safety and process security lies not only in preventing harm, but also in enabling organizations to endure disruptions, whether accidental or intentional, learn from them, and emerge stronger.

SAMENVATTING

“Ik heb de mensen in hun handelen bestudeerd en vastgesteld dat zij allen, zonder uitzondering, slechts één doel nastreven: zich van angst te bevrijden.”

— Ibn Hazm (994–1064)

Dit proefschrift geeft, ten dele, antwoord op die blijvende menselijke zorg. Ibn Hazms reflectie verwijst naar een fundamenteel verlangen naar veiligheid, zekerheid, stabiliteit, vrijheid van schade en, indirect, naar veerkracht. In de chemische procesindustrie (chemical process industry, CPI) kan dergelijke angst niet alleen worden opgevat als een persoonlijk gevoel, maar ook als een weerspiegeling van onzekerheid, kwetsbaarheid en de mogelijkheid van schade als gevolg van ongevallen, kwaadwillende handelingen en operationele verstoringen. Procesveiligheid en procesbeveiliging zijn beide gericht op het verminderen van deze dreigingen, maar worden in de praktijk vaak afzonderlijk beheerd. Dit proefschrift onderzoekt daarom hoe deze domeinen via een veerkrachtgerichte benadering met elkaar kunnen worden verbonden, met als doel chemische installaties niet alleen te helpen verstoringen te voorkomen en te weerstaan, maar zich er ook aan aan te passen, ervan te herstellen en er sterker uit te komen.

De CPI levert een belangrijke bijdrage aan de economische ontwikkeling, maar wordt ook gekenmerkt door gevaarlijke stoffen, complexe technologieën, nauw gekoppelde processen en de mogelijkheid van zware incidenten. Binnen deze context richt dit proefschrift zich op majeure gevaren, ofwel “Type II”-risico’s: relatief zeldzame maar potentieel catastrofale gebeurtenissen, zoals grote branden, explosies, toxische emissies, sabotage, terrorisme en cyberfysieke verstoringen. Hoewel procesveiligheid en procesbeveiliging beide gericht zijn op de bescherming van mensen, activa, operaties en het milieu tegen dergelijke gebeurtenissen, hebben zij zich historisch ontwikkeld als afzonderlijke domeinen, gevormd door verschillende regulatoire tradities, analysemethoden en professionele culturen. Deze scheiding kan leiden tot doublures, onopgeloste afwegingen en blinde vlekken in het beheer van majeure gevaren.

Tegen deze achtergrond luidt de centrale onderzoeksvraag van dit proefschrift: **Hoe kunnen procesveiligheids- en procesbeveiligingsrisicomanagement worden geïntegreerd via een veerkrachtgericht raamwerk voor de chemische procesindustrie?** Om deze vraag te beantwoorden, wordt het proefschrift geleid door vier deelonderzoeksvragen:

1. Wat laat de bestaande literatuur zien over methoden voor procesveiligheid, procesbeveiliging en veerkracht in de chemische procesindustrie, en wat zijn de implicaties daarvan voor geïntegreerd risicomanagement?
2. Hoe beoordelen professionals de integratie van procesveiligheids- en procesbeveiligingsrisicomanagement vanuit een resilience-engineeringperspectief?
3. Hoe kan een resilience-engineeringparadigma worden vertaald naar een geïntegreerde benadering van risicomanagement voor procesveiligheid en procesbeveiliging in de chemische procesindustrie?
4. Hoe kan een veerkrachtgericht raamwerk worden geoperationaliseerd en toegepast in chemische installaties?

Het overkoepelende doel van dit proefschrift is daarom het ontwikkelen en operationaliseren van een veerkrachtgericht raamwerk voor geïntegreerd procesveiligheids- en procesbeveiligingsrisicomanagement in de CPI. Om dit te bereiken, hanteert het proefschrift een multimethodisch onderzoeksontwerp met een sequentiële en cumulatieve logica. Eerst wordt de stand van kennis vastgesteld via een systematische literatuurreview, daarna worden perspectieven uit de praktijk meegenomen via een mixed-methods enquête, vervolgens wordt het raamwerk ontwikkeld via conceptuele synthese, expertinterviews en expert-elicitaties, en ten slotte wordt het raamwerk geoperationaliseerd in twee casestudies in chemische installaties. Dit ontwerp maakt het mogelijk om van probleemanalyse naar conceptuele ontwikkeling en praktische toepassing te gaan, terwijl tegelijkertijd wordt gewaarborgd dat het voorgestelde raamwerk is gebaseerd op zowel theorie als praktijk.

Het proefschrift onderzoekt eerst de gefragmenteerde stand van de bestaande kennis over procesveiligheid, procesbeveiliging en veerkracht. De systematische literatuurreview laat zien dat het veld methodologisch rijk maar conceptueel gefragmenteerd is. Methoden voor procesveiligheid zijn relatief volwassen en worden ondersteund door een breed scala aan gevestigde instrumenten, terwijl methoden

voor procesbeveiligingsbeoordeling en veerkrachtbeoordeling minder ver ontwikkeld zijn. Hoewel sommige methoden veelbelovend zijn voor het omgaan met onzekerheid, onderlinge afhankelijkheden en sociaal-technische complexiteit, behandelen de meeste studies procesveiligheid, procesbeveiliging en veerkracht nog steeds als afzonderlijke of slechts gedeeltelijk verbonden domeinen. Dit bevestigt dat de integratiekloof niet slechts verondersteld wordt, maar duidelijk zichtbaar is in de bestaande literatuur.

Vervolgens onderzoekt het proefschrift de perspectieven van professionals op integratie via een veerkrachtlens. De bevindingen uit de enquête laten zien dat professionals de integratie van procesveiligheid en procesbeveiliging over het algemeen als nuttig en waardevol beschouwen. De meeste respondenten vonden een dergelijke integratie zinvol, met name omdat zij doublures kan verminderen, het gebruik van middelen kan verbeteren en de volledigheid van risicomanagement kan versterken. Tegelijkertijd bleek de steun van professionals voor integratie voorwaardelijk en niet vanzelfsprekend. Belangrijke barrières zijn onder meer beperkte kennis en bewustzijn, onvoldoende middelen, verkokerde communicatie en zwakke coördinatie tussen veiligheids- en beveiligingsfuncties. Daarnaast werd veerkrachtgericht denken overwegend positief beoordeeld, maar bleek de bekendheid met veerkrachtconcepten meestal gering tot matig. Deze bevindingen suggereren dat veerkracht een veelbelovende lens voor integratie kan vormen, maar alleen als zij wordt vertaald naar praktische taal, routines en instrumenten die professionals kunnen herkennen en toepassen. De enquête liet ook zien dat integratie niet alleen een technische kwestie is, maar ook afwegingen tussen waarden en prioriteiten omvat, die per scenario kunnen verschuiven.

Vervolgens ontwikkelt het proefschrift zijn kernbijdrage op conceptueel niveau: het Resilience-oriented Process Safety and Process Security (RoPSS)-raamwerk. Voortbouwend op resilience engineering, expertinterviews en expert-elicitaties stelt het proefschrift dat procesveiligheid en procesbeveiliging niet moeten worden begrepen als parallelle domeinen, maar als gekoppelde sociaal-technische subsystemen binnen een gedeeld landschap van majeure gevaren. Om deze integratie te structureren, is het RoPSS-raamwerk opgebouwd rond vier veerkrachtvermogens: Anticipation, Absorption, Adaptation en Ascension. Deze vermogens zijn ingebed in een zesstappenmanagementcyclus

en gekoppeld aan acht verstoringscategorieën en drie typen prestatie-indicatoren. Op deze manier vertaalt het raamwerk resilience engineering van een abstract perspectief naar een gestructureerde benadering van geïntegreerd risicomanagement voor de CPI.

Een bijzonder belangrijke bijdrage van het proefschrift is de introductie van Ascension als een afzonderlijk veerkrachtvermogen. Waar veel veerkrachtmodellen eindigen bij herstel, respons of leren, betoogt dit proefschrift dat geïntegreerd risicomanagement in de CPI ook een langetermijnvermogen vereist dat herstel, institutioneel leren, continue verbetering, preventie en sterker bestuur omvat. Ascension wordt voorgesteld om deze bredere en meer toekomstgerichte dimensie te weerspiegelen. Daarmee breidt het het veerkrachtdenken uit voorbij onmiddellijk herstel en benadrukt het hoe lessen en herstelervaring kunnen worden vertaald naar sterkere toekomstige prestaties. Dit is vooral relevant voor complexe chemische processystemen waarin accidentele en intentionele verstoringen in de loop van de tijd interacteren met technische voorzieningen, organisatorische routines en governance-structuren.

Daarna richt het proefschrift zich op operationalisering en praktische toepassing. Het RoPSS-raamwerk wordt vertaald naar een gestructureerd semi-kwantitatief instrument en toegepast in twee casestudies in chemische installaties, één in Maleisië en één in Nederland. Deze toepassingen laten zien dat het raamwerk niet alleen als conceptueel model kan functioneren, maar ook als praktisch diagnostisch en sense-makinginstrument. Met gebruikmaking van dezelfde verstoringsgerichte structuur leverden de casestudies basisprofielen van veerkracht op, heatmaps per verstoring en veerkrachtvermogen, samenvattingen per type indicator en kwalitatieve strategieën ter versterking van veerkracht. Hoewel de twee installaties verschilden in context, governance-regelingen, beschikbaarheid van bewijs en toegangscondities, leverden beide toepassingen controleerbare basisprofielen op. Dit suggereert dat het raamwerk voldoende flexibel is om onder realistische industriële omstandigheden gestructureerd te worden toegepast.

Een belangrijke praktische bevinding betreft de behandeling van indicatoren die niet konden worden gescoord. In de casestudies werden sommige items gemarkeerd als “N/A” omdat zij buiten de verantwoordelijkheid op installatieniveau vielen, niet van toepassing waren

binnen de lokale context, of niet met het beschikbare bewijsmateriaal binnen de beschikbare tijdsperiode konden worden onderbouwd. In plaats van deze te beschouwen als eenvoudige ontbrekende data, interpreteert het proefschrift ze als betekenisvolle uitkomsten van de operationalisering die de grenzen van de beoordeling en de governancecondities zichtbaar maken. Dit helpt onderscheid te maken tussen werkelijke tekortkomingen in vermogens en beperkingen die voortvloeien uit scope, verantwoordelijkheid of toegang tot bewijs. Daarmee onderstreept de operationaliseringsfase het belang van grensbewustzijn, traceerbaarheid van bewijs en contextgevoeligheid in veerkrachtgerichte en geïntegreerde beoordeling.

Gezamenlijk laten de bevindingen van het proefschrift een samenhangende ontwikkeling zien. De literatuurreview laat zien dat procesveiligheid, procesbeveiliging en veerkracht gefragmenteerd blijven in de bestaande kennisbasis. De enquête onder professionals toont aan dat integratie gewenst is, maar in de praktijk ook wordt bemoeilijkt. De studie naar de ontwikkeling van het raamwerk reageert op deze behoefte door resilience engineering te vertalen naar het RoPSS-raamwerk. Tot slot tonen de casestudies aan dat het raamwerk in reële chemische installaties kan worden geoperationaliseerd om bruikbare diagnostische uitkomsten en verbeteringsrichtingen te genereren. Overkoepelend concludeert het proefschrift dat een meer geïntegreerde benadering van procesveiligheid en procesbeveiliging in de CPI zowel goed te rechtvaardigen als praktisch haalbaar is, mits deze wordt ondersteund door een veerkrachtgericht perspectief dat de sociaal-technische en governance-aard van systemen met majeure gevaren erkent.

Dit proefschrift levert verschillende theoretische bijdragen. Het verdiept het begrip van procesveiligheid en procesbeveiliging als onderling afhankelijke sociaal-technische subsystemen binnen een gedeeld risicolandschap. Het laat bovendien zien hoe veerkracht kan dienen als organiserend paradigma voor geïntegreerd risicomanagement in de CPI, in plaats van een abstract concept te blijven. Het proefschrift verfijnt ook de veerkrachttheorie door Ascension als een afzonderlijk vermogen te introduceren en door operationele veerkracht en governanceveerkracht binnen één raamwerk met elkaar te verbinden. Daarnaast biedt het een gestructureerde conceptuele architectuur die verstoringscategorieën, veerkrachtvermogens en typen prestatie-indicatoren met elkaar

verbindt, en daarmee een systematischere basis biedt voor geïntegreerd risicomanagement.

Het proefschrift levert ook verschillende praktische bijdragen. Het biedt het RoPSS-raamwerk als een gestructureerde managementbenadering voor de integratie van procesveiligheid en procesbeveiliging. Het biedt een indicatorgebaseerd beoordelingssysteem dat basisprofilering, monitoring en reflectie kan ondersteunen. Het laat zien dat het raamwerk onder verschillende industriële omstandigheden kan worden toegepast en uitkomsten kan genereren die organisaties helpen sterke punten, zwakke punten en verbeterprioriteiten te identificeren. Het benadrukt tevens het belang van verantwoordelijkheidsgrenzen, traceerbaarheid van bewijs en opvolgingsstrategieën in de praktijk van veerkrachtbeoordeling. Naast het gebruik op installatieniveau zijn de bevindingen ook relevant voor toezichthouders, inspecteurs, beleidsmakers en coördinatoren van industriële complexen die op zoek zijn naar meer geïntegreerde en veerkrachtgerichte benaderingen van governance rond majeure gevaren.

Tegelijkertijd erkent het proefschrift verschillende beperkingen. De literatuurreview was begrensd door specifieke inclusiecriteria en heeft mogelijk niet al het relevante opkomende onderzoek omvat. De enquête onder professionals was verkennend van aard en gebaseerd op een relatief kleine, niet-willekeurige steekproef, geconcentreerd in Maleisië en Nederland. De fase van raamwerkontwikkeling moet worden opgevat als expertgeïnformeerd en vormend, en niet als sluitende validatie. Evenzo tonen de casestudies praktische operationalisering en gebruik aan, maar zij bevestigen geen voorspellende validiteit, brede generaliseerbaarheid of effectiviteitsuitkomsten in de tijd. Ook het indicatorsysteem bevindt zich in bepaalde opzichten nog in ontwikkeling, met name wat betreft kwalitatieve beoordeling, interbeoordelaarsconsistentie, beschikbaarheid van bewijs en aggregatiekeuzes. Deze beperkingen doen geen afbreuk aan de waarde van het proefschrift, maar wijzen eerder op het ontwikkelingsstadium van het raamwerk en op de richtingen voor verder onderzoek.

De bevindingen van het proefschrift wijzen ook op verschillende implicaties voor de praktijk en voor toekomstig onderzoek. Voor de praktijk suggereert het proefschrift dat chemische installaties verder moeten gaan dan gescheiden veiligheids- en beveiligingsroutines en sterkere mechanismen moeten ontwikkelen voor gezamenlijke governance,

coördinatie, verstoringsmapping en geïntegreerde doelstellingen. Organisaties zouden veerkrachtgericht denken explicieter moeten opnemen in hun managementsystemen en meer gebruik moeten maken van geïntegreerde indicatoren, terwijl zij tegelijkertijd alert moeten blijven op grenzen van bewijs en verantwoordelijkheidskwesties. Daarnaast is grotere investering nodig in competentieontwikkeling, cross-training, communicatie en langetermijnleren voorbij onmiddellijk herstel. Op beleidsniveau suggereert het proefschrift dat toezichthouders en governanceactoren een sterkere afstemming tussen procesveiligheids- en procesbeveiligingsregelingen zouden moeten bevorderen, met name in opkomende grensoverschrijdende gebieden zoals cyberfysieke dreigingen en governance van industriële clusters.

Voor toekomstig onderzoek beveelt het proefschrift een bredere toepassing van het RoPSS-raamwerk aan in verschillende CPI-contexten, longitudinale studies naar veerkrachtprofielen in de tijd, verdere verfijning van het indicatorsysteem, verkenning van digitale beslissingsondersteunende instrumenten en nadere bestudering van cyberfysieke en grensoverschrijdende contexten. Daarnaast roept het op tot vergelijkende studies tussen RoPSS en gevestigde benaderingen zoals STAMP, FRAM en Bowtie analysis, om te verduidelijken waar RoPSS extra waarde biedt, waar het bestaande methoden aanvult en hoe de veerkrachtgerichte en integratiegerichte kenmerken ervan zich verhouden tot meer gevestigde benaderingen voor het beheersen van gekoppelde veiligheids- en beveiligingsrisico's. Tot slot vraagt het proefschrift om verder onderzoek naar de effectiviteit van het raamwerk, inclusief de vraag of het gebruik ervan leidt tot betere besluitvorming, sterkere veerkrachtprestaties en betere integratie-uitkomsten in de praktijk. Dergelijk onderzoek zou een belangrijke volgende stap vormen in de verdere ontwikkeling van RoPSS als zowel conceptuele als praktische bijdrage aan het vakgebied.

Concluderend behandelt dit proefschrift de langdurige fragmentatie tussen procesveiligheids- en procesbeveiligingsrisicomanagement in de chemische procesindustrie. Het laat zien dat deze scheiding het vermogen van organisaties beperkt om accidentele en intentionele verstoringen op geïntegreerde wijze te begrijpen en te beheersen. Als antwoord daarop ontwikkelt en operationaliseert het proefschrift het RoPSS-raamwerk, dat beide domeinen integreert via de vier veerkrachtvermogens Anticipation, Absorption, Adaptation en Ascension binnen een

zesstappenmanagementcyclus. Door de conceptuele ontwikkeling, de indicatorarchitectuur en de toepassing ervan in twee casestudies in chemische installaties laat het proefschrift zien dat een veerkrachtgerichte benadering zowel een betekenisvolle conceptuele basis als een praktische route kan bieden voor meer geïntegreerd risicomanagement van Type II-risico's in de CPI. Overkoepelend concludeert het proefschrift dat een meer geïntegreerde benadering van procesveiligheid en procesbeveiliging in de CPI zowel goed te rechtvaardigen als praktisch haalbaar is. Uiteindelijk ligt de waarde van een veerkrachtgerichte integratie van procesveiligheid en procesbeveiliging niet alleen in het voorkomen van schade, maar ook in het vermogen van organisaties om verstoringen, of die nu accidenteel of intentioneel zijn, te doorstaan, ervan te leren en er sterker uit te komen.

Chapter 1



Introduction

This chapter introduces the overall problem addressed in the thesis: the continued separation of process safety and process security risk management in the chemical process industry, despite their shared concern with major-hazard risks. It sets out the background, problem statement, research aim, research questions, research design, and main contributions of the dissertation. In doing so, Chapter 1 establishes the need for a resilience-oriented approach that can support a more integrated understanding, assessment, and management of accidental and intentional disruptions in chemical plant settings.

1. INTRODUCTION

1.1 Background

1.1.1 Chemical process industry, process safety, and process security

The chemical process industry (CPI) encompasses plants and facilities that transform raw materials into higher-value products through chemical or physicochemical processes. It includes petroleum refineries, petrochemical complexes, fertilizer and polymer plants, pharmaceutical manufacturing, and other industrial sectors in which chemical processing is central to value creation. Globally, the broader chemical sector has a substantial economic footprint. According to a report prepared for the International Council of Chemical Associations, the global chemical industry directly employed approximately 15 million people in 2017, while its total economic footprint, including supply-chain and induced effects, contributed an estimated USD 5.7 trillion, or about 7% of the world's Gross Domestic Product (ICCA, 2019).

At the same time, the CPI is distinguished from many other manufacturing sectors by three characteristics: large inventories of flammable, toxic, or highly reactive substances; energy-intensive unit operations operating under demanding temperature and pressure conditions; and tightly coupled continuous or high-throughput batch processes. In such settings, a single loss of containment can escalate rapidly into a fire, explosion, or toxic release with consequences that extend far beyond the plant boundary (Mannan, 2012).

The consequences of incidents in the CPI can range from minor workplace injuries to large-scale off-site disasters. Therefore, this dissertation distinguishes between two broad tiers of plant mishaps. Type I risks refer to occupational accidents, such as slips, small fires, or chemical splashes, whose effects are usually confined to the immediate work area. Type II risks, by contrast, refer to rare but potentially catastrophic events, such as vapor cloud explosions, major toxic releases, or acts of sabotage that disable critical protection layers and threaten workers, surrounding communities, supply chains, and the environment (Meyer & Reniers, 2022). This dissertation is concerned specifically with Type II risks, regardless of whether an event originates by accident or through malicious intent.

Within the Type II category, two partially overlapping domains have evolved. Process safety focuses on preventing and mitigating unintentional loss of containment arising primarily from equipment failure, human error, or operational upset. Process security, in contrast, addresses intentional harmful acts, such as sabotage, terrorism, insider action, or cyber-physical intrusion, that seek to exploit chemicals, equipment, systems, or information. Although both domains ultimately aim to protect people, assets, and the environment, they have developed along separate regulatory tracks, rely on different analytical approaches, and are shaped by distinct professional cultures. The result is a set of institutional silos, summarized in Table 1.1, whose reconciliation forms a central concern of this thesis.

Table 1.1: Non-exhaustive list of differences between process safety and process security (adapted from Reniers et al., 2011; Ta et al., 2020)

Dimension	Process safety	Process security
Primary objective	To protect people, assets, and the environment from the hazardous effects of unintentional process-related events	To protect hazardous chemicals, processes, systems, and information from intentional misuse or attack
Nature of incident	Primarily unintentional, such as equipment failure, human error, or operational upset	Primarily intentional, such as sabotage, terrorism, insider action, or cyber-attack
Main concern	Prevention and mitigation of accidental releases, fires, explosions, and toxic exposures across the process lifecycle	Prevention and mitigation of intentional acts that exploit vulnerabilities across the chemical and process lifecycle
Risk expression	Commonly expressed as a function of likelihood and consequence, often supported by historical and quantitative data	Commonly expressed in terms of threat, vulnerability, attractiveness, and consequence, often relying more heavily on qualitative judgement and expert assessment
Analytical basis	Often supported by technical failure data, incident histories, and probabilistic reasoning	Often supported by intelligence, threat scenarios, vulnerability assessment, and expert judgement
Workplace and system design	Tends to favour openness, accessibility, and visibility to support ventilation, safe operation, and emergency response	Tends to favour controlled access, restriction, and protection of sensitive areas, systems, and information
Access to hazardous materials and information	Broader operational accessibility to support safe handling, maintenance, and emergency intervention	Restricted access to authorized personnel on a need-to-know and need-to-access basis
Transparency	High transparency is often encouraged to support learning, reporting, and hazard communication	Disclosure is more tightly controlled to avoid exposing vulnerabilities or sensitive information
Regulatory and guidance anchors	Seveso III, OSHA PSM, IEC 61511, CIMAH Regulations	API 780, Responsible Care Security Code, facility security and cyber-security guidance

Table 1.1 illustrates how process safety and process security can, at times, pull in different operational directions. Process safety generally values transparency, openness, and broad access to information in order to support learning and prevention, whereas process security treats some of the same information as sensitive and requiring controlled access. Even basic design choices may reflect this tension: layouts that support ventilation and emergency response may also increase vulnerability to intrusion, while restrictions intended to strengthen security may complicate safety-related access or communication. If these differences are not carefully reconciled, measures intended to strengthen one domain may inadvertently undermine the other, creating blind spots in the management of major-hazard risks.

Meanwhile, the selected events in **Table 1.2** illustrate how major industrial incidents in the chemical process industry can arise from both unintentional failures and deliberate attacks, and reveal recurring weaknesses in hazard control, emergency preparedness, and organizational oversight. Considered together, these events show that the escalation and consequences of Type II risks are rarely shaped by technical failures alone, but are also influenced by how safety, security, and crisis management arrangements interact in practice.

Table 1.2: Selected major industrial events illustrating key lessons relevant to integrated process safety and process security risk management (mainly extracted from (Meyer & Reniers, 2022))

Year	Event	Nature	Key lessons for integrated risk management
1974	Flixborough (UK) reactor bypass explosion	Safety	Temporary plant modifications require rigorous hazard review and change management.
1976	Seveso (Italy) dioxin release	Safety	Major-hazard management must account for off-site consequences, emergency preparedness, and public communication.
1984	Bhopal (India) methyl isocyanate release	Safety	Poor maintenance, degraded safeguards, and weak emergency planning can turn a process upset into catastrophe.
2005	Texas City (USA) refinery explosion	Safety	Organizational drift, cost pressure, and weak barrier management can erode major-hazard protection.
2005	Buncefield (UK) fuel depot explosion	Safety	Storage and transfer systems can escalate rapidly and produce severe off-site impacts when loss of containment is not controlled.
2010	Deepwater Horizon (Gulf of Mexico) blowout and fire	Safety	Complex operations require robust interface management, barrier assurance, and clear accountability across organizational boundaries.
2013	In Amenas (Algeria) gas plant attack	Security	Physical security and emergency roles must be drilled jointly.
2015	Tianjin (China) warehouse explosions	Safety	Hazardous material storage, escalation control, and effective emergency response are critical in preventing catastrophic off-site consequences.
2015	St-Quentin-Fallavier (FR) truck explosion at gas depot	Security	Routine deliveries can be weaponized; screening is a safety issue.
2017	Triton (Saudi Arabia) malware attack on safety instrumented systems (SIS)	Security	Cyber actors can trigger physical catastrophes through IT/OT convergence.
2019	Abqaiq–Khurais (Saudi Arabia) drone attack	Security	Drone attacks can directly disrupt process operations, showing that physical security threats must be considered alongside process risk.

Taken together, these events suggest that the severity of major-hazard outcomes depends not only on the initiating cause, but also on the ability of a plant to detect weak signals, maintain critical barriers, respond effectively under disruption, and learn from previous failures. This observation points to the importance of a broader performance perspective that cuts across the traditional boundaries of process safety and process security. It also provides a natural bridge to resilience engineering, which offers a useful lens for understanding how chemical plants can prepare for, absorb, adapt to, and improve after both accidental and intentional disruptions.

1.1.2 Resilience engineering

To bridge the divide between process safety and process security, this dissertation adopts the lens of resilience engineering. Resilience engineering reframes risk thinking from how often failures occur to how a socio-technical system can continue functioning under both expected and unexpected conditions. Hollnagel et al. (2012) define resilience as "the intrinsic ability of a system to adjust its functioning prior to, during, or after disturbances so that it can sustain required operations under both expected and unexpected conditions." Leveson (2012) complements this with a control-theoretic perspective, describing a resilient system as one that "continually enforces constraints on behavior even as its structure and environment change," thereby emphasizing dynamic control rather than reliance on static safeguards. Together, these perspectives align well with the dual Type II hazards addressed in the CPI.

Resilience engineering has been further elaborated through several complementary perspectives. Hollnagel et al. (2012) describe resilience in terms of four cornerstones: the ability to anticipate, monitor, respond, and learn. Together, these emphasize that resilient performance depends not only on reacting effectively to disruption, but also on recognizing emerging conditions, maintaining awareness of changing system states, and learning over time. In process safety research, these ideas have also been expressed in terms of plant-level resilience capacities, including anticipation, absorption, adaptation, and restoration capability (Yang et al., 2023; Yarveisy et al., 2022). Anticipation refers to the proactive capability to detect weak signals, monitor emerging threats, and prepare for potential disruptions before they escalate. Absorption refers to the ability of a plant to withstand a disturbance with limited performance degradation. Adaptation refers to the ability to reconfigure resources and responses

as conditions evolve. Restoration concerns the ability to recover and return the system to an acceptable level of functioning (Geng et al., 2023; Yang et al., 2023). For example, recent work on fire-driven escalation has shown how barrier systems can strengthen absorption and adaptation while shortening recovery time (Zeng et al., 2025). Taken together, these perspectives provide a broader performance language that can help bridge the institutional silos between process safety and process security outlined earlier in **Table 1.1**.

This dissertation builds on these resilience perspectives by organizing the proposed framework around four capabilities: Anticipation, Absorption, Adaptation, and Ascension. Ascension is introduced in this research to capture the longer-term dimension of recovery, institutional learning, and continuous performance improvement beyond the immediate restoration of operations. Together, these four capabilities provide the organising logic for the framework developed in this thesis. Table 1.3 presents illustrative examples of how these resilience capabilities may be expressed in process safety and process security contexts.

Table 1.3: Examples of resilience capabilities in process safety and security contexts

Resilience capability	Process safety example	Process security example
Anticipation	Corrosion monitoring identifies early signs of pipe degradation before loss of containment occurs	Threat intelligence identifies emerging interest in stealing or sabotaging hazardous chemicals
Absorption	A blast wall or flameproof enclosure limits the impact of a fire and prevents escalation	A redundant access-control system maintains site security during a power or network outage
Adaptation	Operations are shifted to a safer reduced-capacity mode after failure of a critical heat-exchanger	Security patrol routes and site controls are adjusted in response to a detected drone or intrusion threat
Ascension	Lessons from an incident investigation lead to improved relief-system design and operating procedures	Lessons from an attempted intrusion lead to stronger network segmentation and revised security protocols

Despite its conceptual appeal, resilience engineering remains largely abstract in the CPI. Although quantitative resilience metrics are beginning

to emerge, such as performance-over-time measures for barrier systems, few chemical plants possess a practical roadmap or structured dashboard for assessing whether these four capabilities are in place, let alone integrated across process safety and process security. Developing such a practical and operationally usable framework is therefore a central task of this dissertation.

1.2 Problem statement

The events summarized in **Table 1.2** show that failures rooted in either process safety or process security can spill over into the other domain, transforming what begins as a localized fault or a targeted attack into a major industrial accident. Yet, in many chemical process plants, process safety and process security continue to be managed through separate regulations, organizational structures, and review cycles. This separation can lead to duplication of effort, unresolved trade-offs, and blind spots at the interface between the two domains. For example, practices that support transparency and learning in process safety may conflict with the confidentiality and restricted access often required in process security.

At the same time, the growing complexity of the CPI has increased the need for approaches that go beyond fragmented and purely prescriptive risk management. Existing methods often remain domain-specific, giving limited guidance on how process safety, process security, and resilience can be brought together within a single management approach. Although resilience engineering offers a promising perspective for addressing both accidental and intentional disruptions, it remains difficult to translate into a practical framework for routine use in chemical plants. In particular, there is still limited guidance on how resilience-oriented thinking can be operationalized in a way that reflects practitioner needs, supports integrated decision-making, and can be applied in real plant settings.

This dissertation addresses that gap by focusing on the development and operationalization of a resilience-oriented framework for integrated process safety and process security risk management in the CPI. In doing so, it seeks to move beyond the parallel treatment of safety and security and toward a more coherent approach for understanding, assessing, and improving a plant's capacity to deal with Type II risks.

1.3 Research aim and objectives

The overall aim of this thesis is to develop and operationalize a resilience-oriented framework for integrated process safety and process security risk management in the chemical process industry.

To achieve this aim, the thesis pursues four specific objectives. First, it reviews and synthesizes existing assessment methods related to process safety, process security, and resilience in the chemical process industry. Second, it examines practitioner perspectives on the integration of process safety and process security risk management, including the relevance of a resilience-oriented perspective. Third, it develops a resilience-oriented framework for integrated process safety and process security risk management. Fourth, it operationalizes and applies the proposed framework in chemical plant case studies.

1.4 Research questions

To fulfil the aim of this thesis, one main research question and four tightly scoped sub-research questions are addressed. The main research question provides the overarching direction for the thesis and is framed as follows:

MRQ: ***How can process safety and process security risk management be integrated through a resilience-oriented framework for the chemical process industry?***

This main research question reflects the central problem addressed in the dissertation: although process safety and process security concern the same major-hazard systems, they are still often managed as separate domains in both research and practice. This separation limits the ability of chemical plants to address accidental and intentional Type II risks in a coherent way. The question therefore asks how these two domains can be brought together through a resilience-oriented framework that is not only conceptually meaningful, but also practically relevant to the chemical process industry.

Addressing this question requires a stepwise inquiry into the current body of knowledge, practitioner perspectives, framework development, and operationalization in chemical plant settings. The four sub-research questions below reflect the sequential steps through which this overarching question is addressed.

SRQ1 – Fragmented methods:

What does the existing literature reveal about methods for process safety, process security, and resilience in the chemical process industry, and their implications for integrated risk management?

The first question to be addressed is the fragmented state of existing knowledge. Methods relevant to process safety, process security, and resilience have developed largely along separate lines, with different terminologies, assumptions, and analytical emphases. As a result, there is limited clarity on how far the existing risk assessment methods support integrated risk management, and where important conceptual and methodological gaps remain. This question is therefore necessary to establish the baseline state of knowledge, identify the main approaches used across the three domains, and clarify the extent to which they can support or constrain integration. Answering this question provides the theoretical and methodological foundation for the rest of the dissertation.

SRQ2 – Practitioner insights:

How do practitioners perceive the integration of process safety and process security risk management through a resilience engineering lens?

The second question concerns the practical relevance of integration. Even if an integrated and resilience-oriented approach appears desirable at the theoretical level, it cannot be meaningfully developed without understanding how it is perceived by those involved in managing risk in practice. Practitioners may see clear benefits in integration, but they may also encounter barriers, trade-offs, and competing priorities shaped by organizational routines, regulatory expectations, and sector-specific realities. In addition, resilience-related ideas may be regarded as useful by some practitioners but abstract or unfamiliar by others. This question, therefore, seeks to examine how integration is perceived in practice through a resilience engineering lens, what forms of support or resistance may exist, and what practitioner-informed considerations should shape the development of the proposed framework.

SRQ3 – Framework development:

How can a resilience engineering paradigm be translated into an integrated risk management approach for process safety and process security in the chemical process industry?

This question addresses a central conceptual gap in the dissertation. Although interest in integrating process safety and process security has grown, fragmentation between the two domains continues to limit systemic understanding of industrial risk. In addition, existing theories and methods provide a limited explanation of how coupled safety–security systems evolve under simultaneous constraints, competing values, and both accidental and intentional disruptions. Resilience engineering offers a promising perspective, but its principles are rarely translated into governance structures and risk management approaches that support cross-boundary learning, coordination, and long-term improvement. This question, therefore, focuses on how resilience engineering can be translated into an integrated approach for process safety and process security in the chemical process industry, thereby underpinning the development of the Resilience-oriented Process Safety and Process Security (RoPSS) framework, which serves as the central conceptual contribution of the thesis.

SRQ4 – Operationalization and application:

How can a resilience-oriented framework be operationalized and applied in chemical plant settings?

The fourth problem is practical translation. A conceptual framework alone is not sufficient unless it can be expressed in a form that supports actual use in plant settings. In the present case, this means moving from framework design to a more operational approach that allows resilience-oriented process safety and process security management to be assessed in practice. This requires the development of indicators and an application logic that can be used in chemical plants to generate meaningful insights into strengths, weaknesses, and contextual influences on performance. This question, therefore, focuses on how the proposed framework can be operationalized and applied in practice, thereby connecting the conceptual contribution of the thesis to its use in real industrial environments.

Taken together, these research questions define the intellectual scope and direction of this dissertation. The next section explains how the thesis was designed methodologically to address them.

1.5 Research design

This dissertation adopts a paper-based and multi-method research design (Creswell, 2018), in which the individual studies address interconnected parts of a broader research problem. Rather than presenting the methodology in a standalone chapter, the thesis introduces the overall methodological logic here, while the detailed methods, data sources, and analytical procedures are described in the corresponding paper-based chapters.

This approach reflects the structure of the research, which addresses different aspects of the overall problem through complementary methods. The overall design is sequential and cumulative: it begins by establishing the state of knowledge, then incorporates practitioner perspectives, develops a conceptual framework, and finally operationalizes it in chemical plant settings. In this way, the dissertation moves from problem exploration to solution development and application.

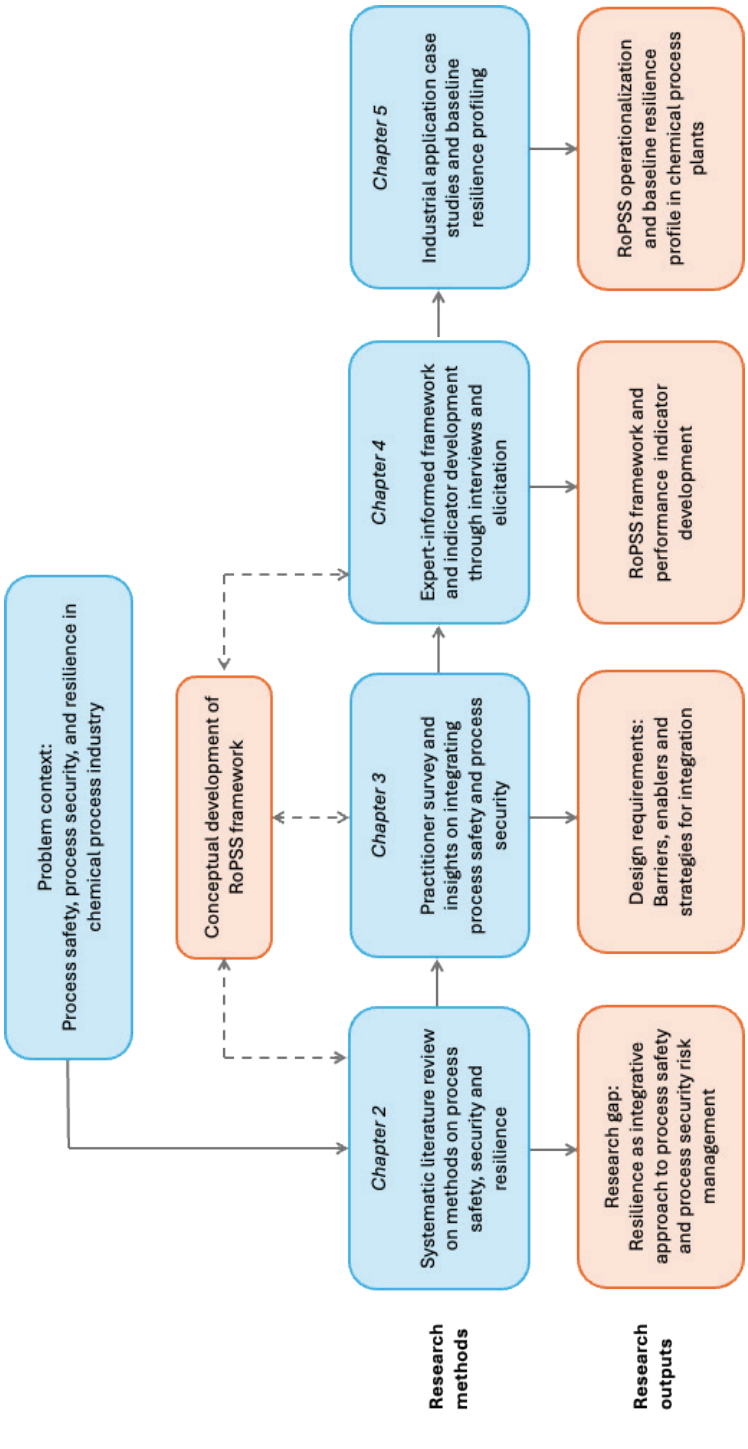

Figure 1.1: Research design and iterative development process of the Resilience-oriented Process Safety and Process Security (RoPSS) framework.

Figure 1.1 summarizes the overall research design and the iterative development process underpinning this dissertation. It shows how the study progresses from problem context and literature-based inquiry to practitioner-informed analysis, conceptual development, and case study application in chemical plants. At the same time, the figure highlights that the research process is not strictly linear, as insights from different stages contribute to the refinement of the RoPSS framework and its indicators. The methodological role of each subsequent chapter is briefly outlined below.

Chapter 2 (based on research paper #1) adopts a systematic literature review design to examine methods relevant to process safety, process security, and resilience in the CPI. The review is conducted using the PRISMA methodology developed by Moher et al. (2009), which provides a structured and transparent process for identifying, screening, and selecting relevant literature. This chapter establishes the theoretical and methodological foundation of the dissertation by synthesizing the existing body of knowledge and identifying the main conceptual and methodological gaps that limit the development of more integrated approaches to process safety and process security risk management.

Chapter 3 (based on research paper #2) adopts a mixed-methods survey design (Zou et al., 2014) to investigate practitioner perspectives on integrating process safety and process security risk management. The survey instrument was partly developed based on the systematic literature review presented in Chapter 2, which identified key conceptual and methodological gaps in existing approaches, and was further informed by related work on integration in the field. Quantitative responses are analysed using descriptive statistics to identify overall patterns in perceptions, while qualitative open-ended responses are analysed thematically using the Thematic Analysis Matrix (TAM) model developed by Zairul (2021). This combination allows the chapter to capture both broad trends and more nuanced practitioner views. In this way, Chapter 3 extends the literature-based insights from Chapter 2 by examining the practical and organizational dimensions of the problem, including perceived benefits, barriers, enablers, value considerations, and strategies associated with integration in real-world settings.

Chapter 4 (based on research paper #3) is primarily conceptual and qualitative in design. It draws on semi-structured interviews with experts from industry, government, consulting, and academia to support the development of the proposed framework. The interview data are analysed using thematic analysis following (Braun & Clarke, 2006), supported by the Thematic Analysis Matrix (TAM) model developed by (Zairul, 2021). In addition, the chapter incorporates expert elicitation and formative assessment principles (Smith & Ragan, 1999) to refine the structure and content of the RoPSS framework and its indicators. Building on the conceptual and methodological gaps identified in Chapter 2 and the practical and organizational insights generated in Chapter 3, this chapter derives the requirements, structure, and resilience-oriented logic of the RoPSS framework as an integrated risk management approach for process safety and process security in the chemical process industry.

Chapter 5 (based on research paper #4) adopts a multiple case study design (Yin, 2017) to operationalize and apply the proposed framework in chemical plant settings. In this stage, the RoPSS framework is translated into a structured set of indicators and applied in two chemical plant case studies, one in Malaysia and one in the Netherlands. The purpose of this chapter is to examine how the framework can be operationalized in practice, generate baseline resilience profiles, and provide initial decision-support insights regarding plant-level strengths, weaknesses, and contextual influences on performance. Accordingly, the case studies are intended to demonstrate the practical applicability and usefulness of the framework in real industrial settings.

Chapter 6 concludes the dissertation by synthesizing the findings from the preceding chapters and reflecting on their implications for research and practice. It revisits the main research question and sub-research questions, consolidates the overall contributions of the thesis, and discusses the extent to which the proposed framework and indicator catalogue are supported through the cumulative findings of the study. The chapter also addresses limitations and outlines directions for future work on integrated and resilience-oriented risk management in the CPI.

Overall, the dissertation combines systematic literature review, survey-based empirical inquiry, qualitative expert-informed framework development, and case study application within a coherent paper-

based structure. This multi-method design is intended to ensure that the proposed framework is informed by both theory and practice, while also showing how resilience-oriented integration can be developed conceptually and translated into an operational approach for chemical plants.

1.6 Contributions

This dissertation makes seven main contributions to research and practice in the field of major-hazard risk management in the CPI.

First, it provides a structured synthesis of methods relevant to process safety, process security, and resilience in the chemical process industry. By reviewing and comparing the existing body of knowledge, the thesis clarifies areas of overlap, fragmentation, and limitation, thereby highlighting the need for a more integrated approach to Type II risk management.

Second, it contributes empirical insight into how practitioners perceive the integration of process safety and process security risk management, as well as the role of resilience in supporting such integration. The survey-based findings reported in Chapter 3 identify perceived benefits, barriers, enablers, value considerations, and practical strategies, thereby grounding the proposed framework in practitioner perspectives and implementation realities.

Third, the dissertation makes a theoretical and conceptual contribution by positioning process safety and process security as interdependent subsystems within a shared socio-technical risk landscape. In doing so, it moves beyond the conventional parallel treatment of the two domains and provides a basis for understanding coupled safety–security interactions, trade-offs, and co-evolving risk dynamics within modern chemical process systems.

Fourth, the dissertation introduces Ascension as a fourth resilience capability. Ascension captures the longer-term dimension of resilience by integrating restoration, institutional learning, governance-level improvement, and continuous performance development beyond immediate recovery. In this way, it extends resilience thinking from

short-term response and restoration toward a more evolutionary and improvement-oriented perspective.

Fifth, the dissertation develops the Resilience-oriented Process Safety and Process Security (RoPSS) framework as an integrated risk management approach for the chemical process industry. The framework brings together process safety, process security, resilience capabilities, governance considerations, and multiple types of disruption within a single conceptual structure, thereby offering a more coherent basis for managing accidental and intentional major-hazard risks.

Sixth, the dissertation operationalizes the proposed framework through a structured set of performance indicators. These indicators translate the conceptual framework into an assessment approach that can support the monitoring and evaluation of resilience-oriented process safety and process security risk management in chemical plants.

Seventh, the dissertation demonstrates the operationalization and usability of the RoPSS framework and its indicators through two case studies in Malaysian and Dutch chemical plants. This application generates baseline resilience profiles for process safety and process security and provides an initial empirical basis for examining the practical usefulness of the framework in plant settings.

Overall, these contributions move the discussion of integrated process safety and process security risk management beyond conceptual separation and toward a more resilience-oriented, theoretically grounded, and operationally usable approach for the CPI.

1.7 Dissertation outline

This dissertation is organized into six chapters. Chapters 2 to 5 form the paper-based core of the thesis and correspond directly to the sub-research questions introduced earlier. Each of these chapters is presented as an article-style manuscript, while Chapters 1 and 6 provide the overall framing and synthesis of the dissertation. **Table 1.4** summarizes the role of each chapter in relation to the research questions and the paper-based structure.

Table 1.4: Dissertation outline

Chapter	Function
1. Introduction	Introduces the background, problem statement, research aim and objectives, research questions, research design, contributions, and overall structure of the dissertation.
2. Mapping the integration gap	Addresses **SRQ1** by reviewing methods relevant to process safety, process security, and resilience in the chemical process industry, and identifies key conceptual and methodological gaps for integrated risk management. (*Paper 1*)
3. Practitioner perspectives	Addresses **SRQ2** by examining practitioner perspectives on the integration of process safety and process security risk management through a resilience engineering lens, with particular attention to practical and organizational considerations. (*Paper 2*)
4. Framework development	Addresses **SRQ3** by developing the RoPSS framework and its indicator architecture through the synthesis of conceptual, methodological, and practitioner-informed requirements. (*Paper 3*)
5. Operationalization and application	Addresses **SRQ4** by operationalizing the proposed framework through indicators catalogue and applying it in two chemical plant case studies to examine practical applicability and generate baseline resilience profiles. (*Paper 4*)
6. Conclusion and outlook	Revisits the **MRQ** and synthesizes the findings of the dissertation, revisits the main research question, reflects on the overall contributions and limitations, and outlines directions for future work.

Although Chapters 2 to 5 are presented as stand-alone article manuscripts and may therefore contain some repetition, this paper-based format allows each study to be read independently while still contributing to a coherent overall thesis. The dissertation now proceeds to Chapter 2, which reviews the existing methods in process safety, process security, and resilience to identify the integration gaps that motivate the subsequent empirical, conceptual, and application chapters.

Chapter 2



Mapping the Integration Gap: Methods for Process Safety, Process Security, and Resilience in the Chemical Process Industry

Chapter 1 set the stage by showing that process safety and process security are often managed through parallel silos, despite their shared concern with major-hazard risks in the chemical process industry. It also argued that resilience engineering offers a useful lens for bridging these domains. The first gap, therefore, is a knowledge gap: what does the existing literature reveal about assessment methods for process safety, process security, and resilience, and how far do these methods support integrated risk management? Chapter 2 addresses this question through a systematic literature review, which maps existing assessment methods across the three domains and identifies the conceptual and methodological gaps that motivate the subsequent chapters.

This chapter is written with modifications based on the following publication: Ab Rahim, M. S., Reniers, G., Yang, M., & Bajpai, S. (2024). Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review. Journal of Loss Prevention in the Process Industries, 88. https://doi.org/10.1016/j.jlp.2024.105274

ABSTRACT

This chapter presents a systematic literature review of risk assessment methods in the chemical process industry (CPI), focusing on process safety, process security, and resilience. Peer-reviewed articles published between 2000 and 2022 were analyzed using the PRISMA methodology, leading to the identification of twelve predominant methods. The findings reveal a shift towards dynamic, systems-based assessment methods, such as the Functional Resonance Analysis Method (FRAM) and the System-Theoretic Accident Model and Processes (STAMP), which are particularly relevant for capturing the complexities of socio-technical systems in the CPI. However, the review also shows that many existing methods place limited emphasis on the resilience paradigm when addressing both process safety and process security risks. Given the evolving challenges of system safety and security threats, there is a clear need for a more holistic approach that integrates process safety, process security, and resilience. This chapter, therefore, highlights opportunities for further research to better prepare the industry for future challenges and to support safer, more secure, and resilient operations.

2. MAPPING THE INTEGRATION GAP

2.1 Introduction

2.1.1 Context

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

Although the majority of workplace accidents are caused by Type I risks, which are occupational accidents (such as falls and small fires) and minor security events (such as petty theft), Type II risks, which are major accidents or incidents can result in a catastrophic event, also frequently occur with numerous fatalities and major asset damages. To help readers better grasp the focus of this study on Type II risk, we have laid out the differences in risk types between safety and security in **Table 2.1**.

Table 2.1: Comparative overview of the type of risk between safety and security (Moreno et al., 2018; Landucci et al., 2020; Meyer & Reniers, 2022)

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

Notes: E = events; C = consequences; L = likelihood

Actually, from a global viewpoint, Type II incidents happen semi-regularly, including major fires, explosions, and large toxic releases (Meyer & Reniers, 2022). Notable process safety-related accidents include the Flixborough disaster (1974), the Bhopal gas tragedy (1984), the Texas City refinery explosion (2005), and the Deepwater Horizon catastrophe (2010), which were caused by safety-related factors such as inadequate safety measures, insufficient training, and/ or poor maintenance (Amyotte et al., 2016; Kleindorfer et al., 2012). These incidents highlight the importance of robust process safety risk assessment methodologies, such as Hazard and Operability Study (HAZOP), Layer of Protection Analysis (LOPA), and Quantitative Risk Assessment (Pasman et al., 2009).

Unlike safety-related accidents, however, security-related events are intentional and sometimes well-planned. Process security-related events may also cause harm to human health, loss of life, and major asset damage. Incidents such as the Saudi Aramco drone attacks (2019) and the Toulouse

fertilizer plant explosion (2001)[1]emphasize the need for effective process security risk assessment and management to better protect CPI facilities against external threats, such as theft, sabotage, or acts of terrorism (Aven, 2007). Various techniques have been proposed and applied in the CPI context, including the Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF), and API Security Vulnerability Assessment Methodology (Matteini et al., 2019).

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

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

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

Meanwhile, applying the resilience engineering paradigm is gradually being explored as an approach to provide a safety net in CPI (Jain et al., 2018; Pasman et al., 2020a; Yarveisy et al., 2022). In the broad sense, resilience is a system's ability to maintain or achieve desired functionality following some event (Logan et al., 2022). In resilience engineering, a system is said to be resilient if it can adjust its functioning before, during, or following changes and disturbances and sustain required operations under expected and unexpected conditions (Hollnagel, 2006). Resilience engineering aims to enhance a system's capabilities to absorb, adapt, and recover from disruption and reduce the impacts of the disruptions on the system's performance (C. Chen et al., 2023; Hosseini et al., 2016a). Therefore, the process resilience concept not only focuses on reducing the likelihood and consequence of failures but also on enhancing the system's ability to absorb and recover from shocks. It goes beyond traditional risk management by considering how quickly and effectively an organization can adapt to unexpected changes or recover from disasters (Hickford et al., 2018; Jain et al., 2018a). Currently, several resilience assessment methodologies have been proposed and developed for managing socio-technical systems in the face of uncertainties, disturbances, and potential hazards in the CPI context, such as the Functional Resonance Analysis Method (FRAM), Process Resilience Analysis Framework (PRAF) and STAMP-based Quantitative Resilience Assessment (Jain et al., 2018b; Patriarca et al., 2017; Sun et al., 2022).

2.1.2 Need for this review

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

further, emphasizing the need for an integrated approach to managing process safety, process security, and resilience in the CPI.

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

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

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

accidents and deliberate attacks, ensuring the sustainability and resilience of the CPI in the long run.

2.1.3 Aim and scope of the review

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

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

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

The structure of this chapter is organized as follows: Section 2 outlines the methodology adopted for the systematic literature review (SLR), detailing the search strategy implemented. Section 3 presents the findings of our SLR, offering an overview of the fundamental concepts associated with process safety risk assessment, process security risk assessment, and resilience assessment within the CPI. This section further delves into the diverse approaches and stages of application of these assessment methods

in the CPI context. Section 4 engages in a critical discussion, evaluating the strengths and limitations of these methodologies, especially when addressing process safety and process security risks, and resilience in the CPI. Subsequently, the chapter identifies promising trajectories for future research in these domains. Lastly, Section 5 presents the conclusions and recommendations for subsequent research efforts.

2.2 Methodology

2.2.1 The review protocol

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

2.2.2 Formulation of the research question

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

2.2.3 Systematic searching strategies

To identify relevant studies, the study's keywords were utilized in a search that was derived from the research question. These keywords included process safety and process security, risk assessment and resilience assessment, and the chemical process industry. To increase the relevance of results for the review, the search process employed synonyms,

associated terms, and variations. Moreover, the identification procedure was informed by previous studies and keywords suggested by the selected database and industry experts. A complete search string was then developed, utilizing various search techniques, such as Boolean operators, phrase searching, truncation, wild cards, and field code functions, on the two primary databases, Web of Science (WoS) and Scopus. The search string for both databases is as follows: ((("process safety" OR "process security" OR "physical security") AND ("risk assessment" OR "risk analysis")) OR ("resilience assessment" OR “resilience analysis”)) AND ("chemical industr*" OR "process industr*" OR "chemical plant*" OR "process plant*" OR “chemical facilit*” OR “process facilit*”). The search was conducted on March 14th, 2023, generating a total of 713 documents, which consist of 282 from WoS and 431 from Scopus, as demonstrated in **Figure 2.1**.

2.2.4 Screening

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

During the screening phase, it was noted that the number of studies on process safety, process security, and resilience risk assessment methods has steadily increased since 2000. However, this study did not include articles published in 2023 (N = 8) during the search because a whole year was not completed. Consequently, articles published between 2000 and 2022 were selected as one of the inclusion criteria for this study. To minimize misunderstanding, the review incorporated only articles published in English. Other inclusion and exclusion criteria are listed in **Table 2.2**. Both records from WoS and Scopus were then amalgamated in the Zotero, 2023 reference manager, and duplicate articles were removed in this process. We then carefully screened the records by title, abstract,

and keywords corresponding to our criteria, resulting in 129 remaining articles being deemed eligible for the subsequent review stage.

Table 2.2: Inclusion and exclusion criteria for the screening and eligibility process

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

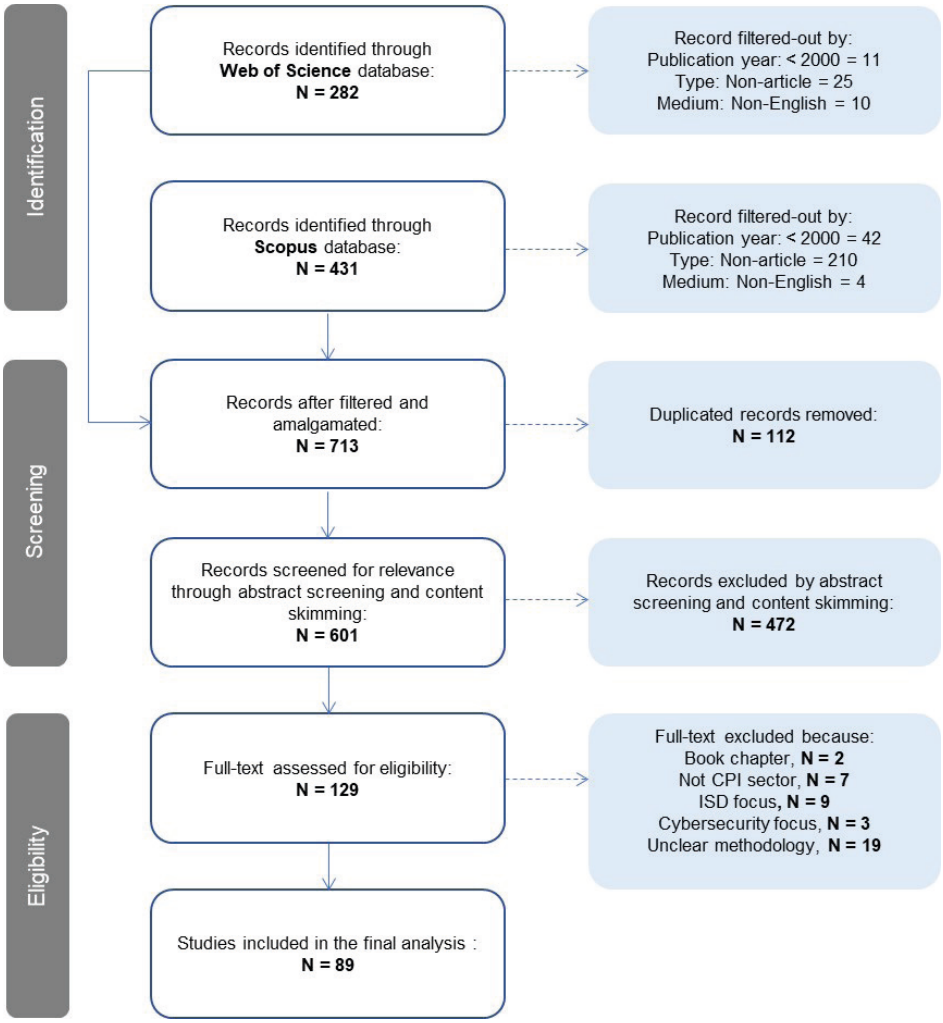

Figure 2.1: Systematic literature review flowchart. Adapted from PRISMA 2020 Method.

2.2.5 Eligibility

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

2.2.6 Data extraction and analysis

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

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

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

2.3 Results

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

Our search yielded 713 results, and after careful screening, we included 89 peer-reviewed articles in our study. **Table 2.3** summarizes the most prominent publication titles, authors, and countries in process safety, process security, and resilience assessment research.

Table 2.3: Top 10 record count according to publication titles, authors, and countries

Publication Titles	JCR Quartile[1]	JCR IF 2022	Record Count	Authors	Record Count	Countries	Record Count
J. of Loss Prevention in the Process Industries	Q2	3.5	23	Khan F	12	USA	25
Process Safety & Environmental Protection	Q1	7.8	12	Mannan MS	8	Canada	13
Process Safety Progress	Q4	1.0	12	Yang M	7	P.R. China	10
Reliability Engineering & System Safety	Q1	8.1	9	Jain P	6	India	9
Safety Science	Q1	6.1	7	Reniers G	6	Netherlands	9
Computers & Chemical Engineering	Q2	4.3	6	Cozzani V	4	Italy	8
Journal of Hazardous Materials	Q1	13.6	6	Gupta JP	4	Kazakhstan	5
IEEE Access	Q2	3.9	2	Bajpai S	3	Belgium	4
Sustainability	Q2	3.9	2	Moreno VC	3	Greece	4
Chemical Engineering Science	Q2	4.7	1	Pasman HJ	3	Norway	4

Notes:
JCR = Journal Citation Reports (JCR, 2023); IF = Impact Factor
1 Highest quartile in a relevant JCR category

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

research in this area. Overall, the elevated Impact Factors and strong JCR quartile rankings of these journals highlight the rigor and significance of the ongoing research in this field.

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



Figure 2.2: Distribution of papers published between 2000 to 2022 across four domains

As shown in **Figure 2.2**, from 2000 to 2022, the publication landscape related to chemical process industry reveals evolving research priorities. Process safety has consistently maintained focus throughout, with publications gradually growing, particularly from 2017 onwards. This surge may be influenced by factors like increasing industrial complexities, and evolving safety standards and regulations. On the other hand, the process security's publication trend appears to be more sporadic, with initial activities in the early 2000s followed by a dormant period, hinting that the security aspect might have been relatively under-researched. However, only in 2019, a focus on integrating process safety and process security risk assessment in this sector started to emerge, indicating a newfound recognition of the importance of intertwining safety and security for comprehensive process plant protection.

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

2.3.2 Overview of process safety risk assessment, process security risk assessment, and process resilience assessment methods

Risk assessment is a systematic process of understanding the nature of risk and evaluating the potential risks that may be involved in a projected activity with the available knowledge (Bjørnsen et al., 2020; SRA, 2018). It is the process used to understand the nature and determine the risk level by analyzing potential hazards and evaluating the possible impacts of occurrence. ISO 31000: 2018 provides a framework for risk management that is widely accepted and implemented across many sectors, including the CPI. Our review focuses on the first two stages of risk assessment (**Figure 2.3**), part of this generic framework, which involves risk identification and risk analysis (estimation of consequences and likelihoods and risk calculation).



Figure 2.3: Overview of risk management process (ISO 31000: 2018)

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

by the likelihood (probability in quantitative terms) of an event and its severity of consequences. Put simply, **Process safety risk = Probability x Consequence** (Adedigba et al., 2018; B et al., 2020; Guo et al., 2018).

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

As highlighted by Landucci et al. (2020) and Matteini et al. (2019), systematic methodologies for process safety risk assessment have been developed over the past forty years to address the growing complexity within the CPI, culminating in established practices like dynamic Quantitative Risk Assessment (QRA). In contrast, the evolving nature of Type II process security risks has not been as thoroughly addressed, as process security risks can shift dramatically based on unpredictable socio-political events. The effort of evaluating risks associated with potential terrorist attacks on industrial sites is especially complex for several reasons. Firstly, there is a limited historical precedent of terrorist activities targeting chemical process installations. Secondly, a multitude of external elements can either amplify or mitigate these security risks. Lastly, the factors that influence these security (and safety) risks are not static; they interact in a dynamic manner and evolve over time, as noted by Landucci et al. 2020) and Moreno et al. (2018).

Therefore, the early literature on process security risk assessment largely presents speculative and qualitative insights. Historically, the emphasis on this subject grew after the 9/11 attacks, leading to the creation of Security Vulnerability Assessment (SVA) methods by the American Petroleum Institute (API) and Center for Chemical Process Safety (CCPS), both first published in 2003. CCPS (2003) defines security risk as the likelihood of an adversary or threat successfully exploiting a specific vulnerability of a particularly attractive target, resulting in a degree of damage or impact

on an asset. Similarly, the ANSI/API Standard 780 defines security risk as a “function of the Consequences of a successful attack against an asset and the Likelihood of a successful attack against an asset” (Moore, 2013). As explained by (Landucci et al., 2020), the “likelihood of a successful attack” can be equated to vulnerability (V). Additionally, the anticipated consequences can be viewed as a blend of the “attractiveness of the asset to the threat” (A) and the "threat" (T) parameter. This is because the greater the anticipated consequences, the more enticing an asset becomes to a potential adversary, increasing its threat level. Moreover, Consequence (C) denotes the “worst-case consequences” or the impact value associated with the security risk. Put simply, **Process security risk = V x (A x T) x C**.

Progressively, there are a handful of semi-quantitative methodologies that have been

introduced or utilized in real-world scenarios for process security risk assessment across various facilities. Common factors considered in these methodologies encompass threat levels, the attractiveness of the facilities to adversaries, potential consequences and repercussions of an incident, and the vulnerability level (Bajpai & Gupta, 2005). While there are subtle variations across different methodologies, a general step-by-step procedure is discernible, which encompasses the primary stages outlined in **Table 2.4**.

Table 2.4: SVA methodologies for the chemical and petrochemical industry (adapted from (Landucci, Khakzad, & Genserik, 2020; Matteini et al., 2019)

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

However, Reniers et al. (2020) argue that process safety and process security are intertwined, the only difference being the human intention of causing the losses. As illustrated in **Figure 2.4**, they explain that, in process safety, a protection or prevention barrier is required to prevent a hazard or threat from reaching the target. Meanwhile, in process security, a countermeasure is required to prevent a threat from becoming out of control.

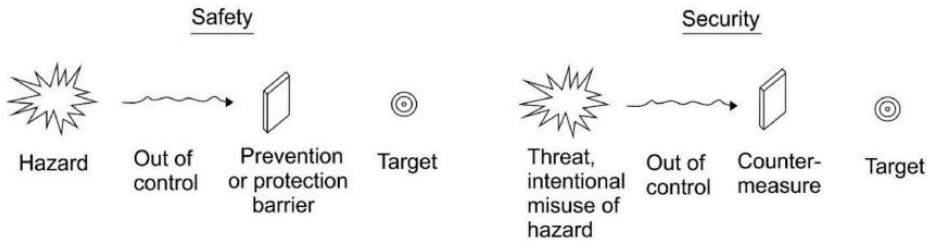

Figure 2.4: Constitutive elements of process safety risk and process security risk (Reniers et al., 2020)

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

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

recover from unexpected disruptions through the implementation of appropriate measures (C. Chen et al., 2021; Vairo et al., 2020).

However, Jain et al. (2018a) point out that process systems resilience needs to be more standardized and quantifiable. Drawing inspiration from Hollnagel's foundational principles of resilience engineering (anticipation, monitoring, response, and learning), (Jain et al., 2017) outlined four elements for a process resilience analysis framework. These elements encompass early detection (spotting weak signals via vigilant monitoring and anticipation), error-tolerant design designs that are forgiving to errors (incorporating inherently safer design principles), plasticity (often described as resistive adaptability), and recoverability, as shown in **Figure 2.5**.

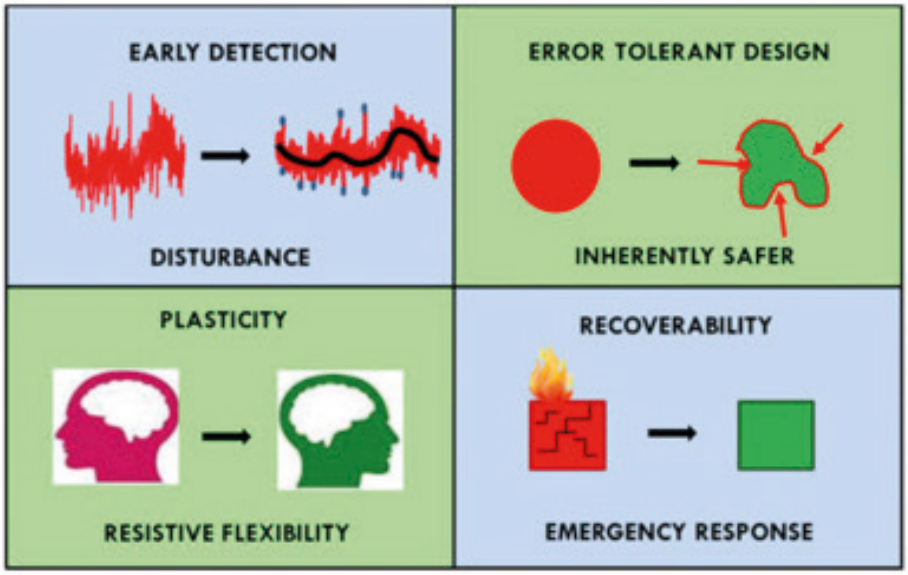

Figure 2.5: Elements of process resilience (Jain et al., 2017)

To this point, there are similarities and differences between process safety risk assessment, process security risk assessment, and resilience assessment, as summarized in **Table 2.5**. Process safety risk Assessment primarily focuses on managing risks associated with accidents resulting from unintentional events, such as equipment failure, human error or human violations. For instance, Process Hazard Analysis (PHA), often conducted using methods like HAZOP, is an essential step in identifying

potential hazards and mitigating the associated risks (Chastain et al., 2017; J. Y. Choi & Byeon, 2020; Venkatasubramanian et al., 2000). This approach has a well-established process for defining risk tolerance criteria, identifying hazardous scenarios (mainly static), and applying a probabilistic perspective to calculate risks. An example might be identifying a potential equipment failure that could lead to a chemical leak and then designing safety measures such as redundancy or automatic shut-off systems to prevent this scenario (Marhavilas et al., 2020; Penelas & Pires, 2021; Ramzan et al., 2007).

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

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

Table 2.5: Comparison between process safety risk assessment, process security risk assessment, and resilience assessment (Baybutt, 2017; Reniers et al., 2020; Varadharajan & Bajpai, 2023; Yang et al., 2023)

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

Despite their distinct focus areas, these three assessment methods share a common goal: safeguarding CPI's operations from risks, whether unintentional or deliberate, and ensuring the system's resilience amid unforeseen challenges. By complementing each other, they together provide a comprehensive, multi-faceted approach to risk management in the CPI. Therefore, understanding their unique contributions and

limitations can lead to a more robust and resilient chemical process industry.

2.3.3 Type of approach, tools, and stage of assessment

Our comprehensive analysis, as in **Appendix A**, has categorized the assessment methods into three distinct categories: qualitative, quantitative, and semi-quantitative. The distribution of these approaches across different assessment areas is visually represented in **Figure 2.6**.

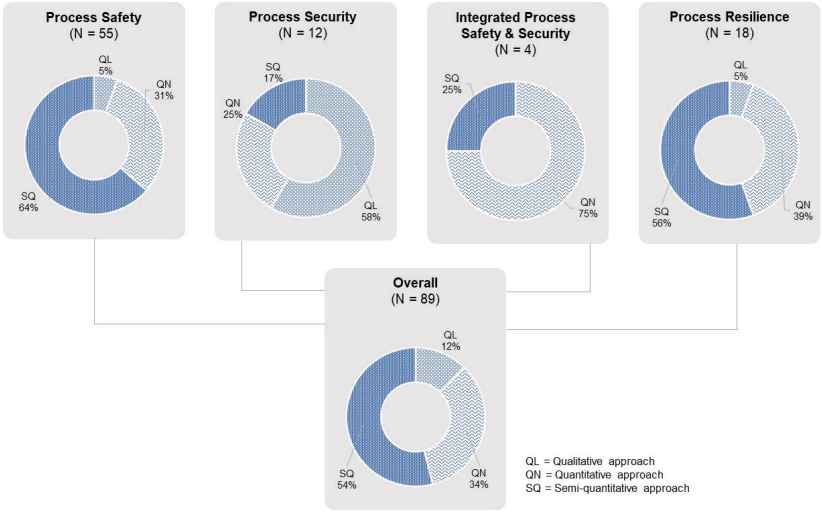

Figure 2.6: Distribution of assessment approach across different domains

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

Conversely, the quantitative approach, which makes up 34% overall, is rooted in mathematical models and statistical analyses. It seeks to quantify risks based on empirical data, making it especially relevant in areas flush

with data and where risks can be numerically articulated. A notable observation is the integrated process safety and security domain, where 75% of its methods are quantitative. This suggests a pronounced tilt towards data-driven assessments when jointly considering safety and security. However, it is crucial to note that the sample size for this domain is relatively small (N=4), which might limit the robustness of this observation.

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

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

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

Protection Analysis (LOPA) and Bayesian Networks, which seamlessly blend qualitative insights with quantitative rigor.

To provide a clearer perspective, we have crafted a visual representation depicted in **Figure 2.7**, showcasing the diverse techniques or tools favored by researchers across the domains under scrutiny. It is worth noting that the circle size in this representation is proportionate to the number of studies within each domain. Within the process safety domain, predominant techniques encompass Hazard and Operability Study (HAZOP), Bayesian Networks (BN), Fault Tree Analysis (FTA), Bowtie, and Layer of Protection Analysis (LOPA). In the domain of process security, techniques such as Security Vulnerability Assessment (SVA) and risk matrix find frequent applications. When researchers develop integrated process safety and security risk assessment methods, the techniques are mainly combinations of BN, FTA, and Event Tree Analysis (ETA). Meanwhile, in process resilience assessment, the spotlight is on methods rooted in the BN, Functional Resonance Analysis Method (FRAM), Process Resilience Analysis Framework (PRAF), Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA), and System-Theoretic Accident Model and Processes (STAMP).

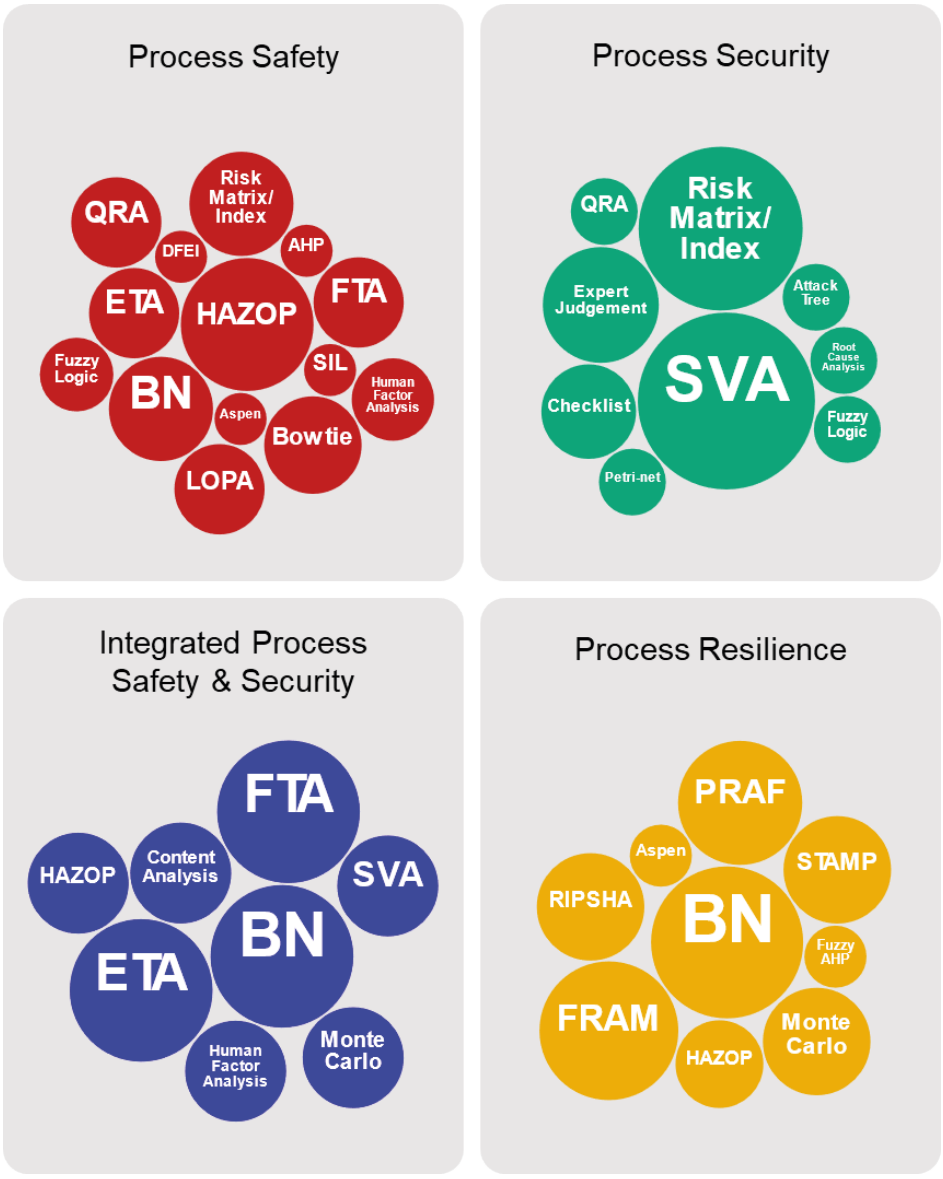

Figure 2.7: Main process safety and process security risk, and process resilience assessment techniques employed in the CPI (the size of the circle is relative to the number of studies in the same domain)

Diving deeper, the assessment stage of these assessment methods can vary depending on the specific needs and objectives of the studies. We have dissected how those studies deploy the assessment methods at

different stages, including hazard identification, likelihood or vulnerability analysis, consequence analysis, and overall risk calculation or estimation.

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

2.4 Discussion

2.4.1 Strengths and limitations of process safety, security, and resilience assessment methods

Our analysis, building on the results from the previous sections, highlights that methods such as BN, Bow-tie, ETA, FRAM, FTA, HAZOP, LOPA, PRAF, RIPSHA, Risk Matrix, STAMP, and SVA are frequently employed to address concerns related to process safety, process security and/or process resilience in the CPI. In this section, we further analyze the strengths and limitations of these 12 methodologies and their applicability within the process safety, process security, and process resilience domains. The insights are summarized in **Table 2.6**.

The diverse methodologies and tools available for risk assessment in the CPI underscore the industry's multifaceted nature and the challenges it faces. The choice of method often reflects the specific challenges and objectives of a given study or application. For instance, while HAZOP is a mainstay for hazard identification in process safety, its limitations in addressing intentional security threats highlight the need for more specialized tools in the process security domain. The prominence of semi-quantitative methods, as evidenced in our earlier analysis, suggests a broader industry preference for a balanced approach. This balance, which

combines the rigor of quantitative data analysis with the flexibility and context provided by qualitative expert judgment, is particularly relevant in an industry where risks can be both well-defined and highly unpredictable.

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

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

Table 2.6: Analysis of strengths and limitations of main assessment methods for addressing process safety (Safe.), process security (Sec.), and resilience (Res.)

Method	Strengths	Limitations	Applicability			Main References
			Safe.	Sec.	Res.	
Bayesian Network-based	Incorporates prior knowledge even with sparse data. Dynamic risk assessment suitable for analyzing complex CPI systems. It can be updated in real time or as new info becomes available.	Sensitive to choices of prior probabilities. Heavy computational requirements, especially for large systems. May face challenges in validation and verification.	x	x	x	(Amin et al., 2022; Baksh et al., 2015; Kanes et al., 2017; Roy et al., 2014; Song et al., 2019)
Bow-tie-based	Visual representation of relationships between hazards and threats. A comprehensive approach to both intentional and unintentional threats. May integrate resilience engineering concepts.	Might overlook certain scenarios. Relies on expert judgment and estimations. May miss interdependencies between different bow-ties.	x			(B et al., 2020; Guo et al., 2018; Santana et al., 2022; Schmitz et al., 2021)
ETA-based	Systematic visualization of event sequences. Quantifies the probability of different outcomes. Useful for understanding the progression of events.	Requires a clear initiating event. It may not capture all possible event sequences. Relies on accurate probability data for each event.	x	x		(Chen et al., 2020; Fang et al., 2020; Kim et al., 2003; Moreno et al., 2022)

FRAM-based	Focuses on variability and performance in systems. Highlights the impact of variability on safety and security. Aligns with resilience through adaptability focus.	Requires a deep understanding of system functionality. Its qualitative nature can be complex to incorporate in traditional methods. Limited practical implementation examples.	x	x	x	(Bjørnsen et al., 2020; Menezes et al., 2021; H. J. Pasman et al., 2018; Yousefi et al., 2019; Zinetullina et al., 2021)
FTA-based	Graphical representation of the combinations of failures leading to an undesired event. Quantitative method that can calculate the probability of the top event. Helps in identifying the root causes of failures.	Can be complex for large systems. Requires accurate and comprehensive failure data. It might not capture dynamic interactions in the system.	x	x		(Aneziris et al., 2014, 2017; Krishna et al., 2003; Sano et al., 2020)
HAZOP-based	Comprehensive identification and analysis of potential hazards. Fosters interdisciplinary cooperation for a thorough assessment. Highly systematic, ensuring comprehensive coverage of failure modes.	Less precise for processes with intricate relationships. Struggles with identifying intentional security threats. Focuses on individual events over combinations.	x			(Ávila et al., 2013; Bartolozzi et al., 2000; Penelas & Pires, 2021; Ramzan et al., 2007)

LO-PA-based	Excellent for simplifying, quantifying, and prioritizing risk, providing a clear view of safety measures required. Facilitates risk communication between different stakeholders.	Less suitable for handling the unpredictable and qualitative nature of security threats, Relies heavily on quantitative risk data.	x		(Chastain et al., 2017; Wagner & Champion, 2012; Wasileski & Henselwood, 2011)
PRAF	A holistic method combining technical and social factors. Enhances resilience and encourages a proactive safety culture. Provides quantitative assessment using plant performance data.	Lacks comprehensive comparison with other methods. It might be computationally expensive for large systems. Assumption constraints like the normal distribution of uncertain parameters.	x	x	(Jain et al., 2019; Jain et al., 2018a; Jain et al., 2019; H. Pasman et al., 2020b)
RIPSHA	Integrative method capturing technical, human, and organizational factors. Grounded in resilience engineering. Adaptable across chemical process plant life cycles.	It might be resource-intensive and demanding. There is no quantitative comparison with other hazard analysis methods. Requires extensive data collection from varied sources.	x	x	(Jain et al., 2018; Jain, et al., 2018c; Pasman et al., 2020b)

Risk Matrix / Index-based	Rapid qualitative tool for prioritizing process safety risks. Facilitates clear communication of risk. It can be used for the initial screening of security risks.	Potential oversimplification of security threats. Might not grasp the dynamic nature of threats. Relies on qualitative and subjective assessments.	x	x		(Bajpai & Gupta, 2007; Baybutt, 2017a; Dunbobbin et al., 2004; Moore, 2006)
STAMP-based	Views accidents as system failures, not just components. Comprehensive in addressing human, organizational, and technical factors. Strong for understanding resilience with a system-wide perspective.	Lacks a formal mathematical foundation. It may be subjective and qualitative in nature. May miss specific vulnerabilities in large-scale systems.	x	x	x	(Cameron et al., 2017; Pasman et al., 2018; Sun et al., 2022)
SVA	Comprehensive evaluation of potential security threats. Identifies vulnerabilities and suggests countermeasures. Integrates both technical and human factors	It might be subjective based on the expertise of the assessor. Requires regular updates as threat landscapes evolve. It may not capture all potential vulnerabilities.		x		(Bajpai & Gupta, 2005; Lemley et al., 2003; Moore, 2006)

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

BN-based methods excel in managing uncertainty and complexity, which is essential for addressing safety, security, and resilience. BN's graphical models offer clear visualization of causal relationships, and its probabilistic nature facilitates informed decision-making amidst uncertainty. While BN's dynamic risk management capability is advantageous for the ever-evolving

CPI landscape, its data-intensive nature and the need for specialized expertise can be limiting, especially when relevant data is scarce.

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

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

RIPSHA, grounded in sociotechnical systems, offers a holistic approach to process safety and potential process security. It captures the nuances of modern socio-technical systems, emphasizing interactions and interdependencies. While RIPSHA integrates resilience engineering concepts, its reliance on expert judgment and the need for extensive data are areas of concern.

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

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

approach, capitalizing on their strengths and addressing their weaknesses, could be the key to effective risk management in this dynamic sector.

2.4.2 Future Research

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

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

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

Thus, future research should prioritize the exploration and integration of resilience principles into process safety and process security assessment methodologies. This research direction necessitates the establishment of clear, quantifiable metrics for measuring resilience that can be seamlessly integrated into comprehensive process safety and security risk assessment tools. Importantly, these tools should incorporate decision-making elements to guide operators and regulators in prioritizing interventions. It also calls for in-depth case studies to glean insights into the successful (or

unsuccessful) real-world applications of resilience principles. Furthermore, there is a pressing need to create or refine tools that not only assess risks but also offer actionable insights on bolstering system resilience. Lastly, it is imperative to ensure that industry professionals receive adequate training and education, equipping them with the requisite knowledge and skills to weave triplets of process safety, process security, and resilience strategies into their operations. By addressing this literature gap, the CPI can move towards not just safer and more secure operations but also systems that are robust, adaptable, and resilient in the face of an ever-evolving landscape of risks and challenges.

2.5 Conclusion and recommendations

In the CPI, ensuring effective process safety, process security, and resilience is paramount. This review has highlighted a significant gap in the current literature. There is a notable absence of studies integrating the resilience paradigm into a cohesive framework for process safety and process security risk assessment and management. Addressing this gap is important for supporting a more comprehensive approach to risk management that aligns with the dynamic nature of the CPI and contributes to a high level of protection for people, assets, and the environment. While the findings highlight the growing importance of resilience measures in the CPI, it is imperative to reiterate that these measures should complement, not replace, the thoroughness of risk assessments. Rigorous risk assessment remains the cornerstone of effective resilience-oriented management, ensuring a comprehensive understanding of potential hazards, threats, and vulnerabilities, and supporting informed decision-making.

Drawing from this review, chemical industries are encouraged to embed systems-based semi-quantitative assessment techniques within their safety, security, and resilience practices. Such techniques strike a balance between quantitative data and qualitative expert judgment, aptly suited for the complex and dynamic risk environments inherent to the CPI. Unlike purely qualitative or quantitative methods, semi-quantitative approaches can adeptly capture both the uncertainty and variability of risk factors and the dynamic nature of process systems, offering a more realistic basis for assessment.

Furthermore, holistic management of process safety and process security risks requires the development and adoption of unified frameworks.

Such frameworks can support a more comprehensive and integrated risk management strategy, encompassing both safety and security dimensions, while also incorporating resilience-oriented thinking. A unified framework should not only support risk assessment but also guide decision-making processes for enhancing system resilience. Organizations, therefore, need to encourage continuous learning and adaptive strategies in light of the dynamic nature of process safety and process security risks. This commitment can manifest in joint safety and security audits, incident investigations, and periodic revisions of risk assessment frameworks and management to ensure their continuing relevance and effectiveness.

There is also a pressing need to further research to refine system-based semi-quantitative approach and examine how they can be integrated into broader risk management frameworks. Such endeavors can provide the process industry with improved tools and strategies for addressing process safety, process security, and resilience challenges.

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

Chapter 3



Practitioner Perspectives on Integration: Process Safety, Process Security, and Resilience Engineering in Practice

Chapter 2 established that existing assessment methods for process safety, process security, and resilience remain unevenly developed and only partially integrated. While this literature-based finding clarifies the knowledge gap, it does not fully explain how integration is perceived by those responsible for managing risks in practice. Chapter 3, therefore, turns to practitioners. Using a mixed-methods survey, it examines how professionals perceive the usefulness of integrating process safety and process security risk management, their awareness of resilience-oriented thinking, the values and trade-offs involved, and the barriers, enablers, and strategies that may shape practical implementation.

This chapter is written with modifications based on the following publication: 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

ABSTRACT

This chapter examines how practitioners perceive the integration of process safety and process security risk management in the chemical process industry, with particular attention to the role of resilience-oriented thinking. A mixed-methods approach was applied, combining quantitative survey data from 47 industry professionals with qualitative insights from open-ended responses. The findings highlight several perceived advantages of integration, including optimized resource use, reduced operational redundancies, and improved risk management. However, barriers such as knowledge gaps, resource constraints, and communication silos were also identified. Respondents emphasized the importance of proactive risk management, continuous improvement, adaptability, and stronger coordination between safety and security practices. Critical enablers for integration include leadership commitment, alignment with societal values, cross-disciplinary training, and integrated risk assessment and management. Emerging technologies and regulatory alignment were also identified as relevant factors in facilitating integration. The chapter contributes to the thesis by providing practitioner-informed insights into the perceived value, practical feasibility, barriers, enablers, and strategies associated with integrating process safety and process security risk management through a resilience-oriented lens. These insights lay the groundwork for the resilience-oriented framework developed in the following chapter.

3. PRACTITIONER PERSPECTIVES ON INTEGRATION

3.1 Introduction

The chemical process industry (CPI) is characterized by complex operations that involve processing chemicals into a wide range of products and materials essential to various sectors, such as petrochemicals, pharmaceuticals, and agriculture. To manage the inherent risks in such operations, the CPI has historically prioritized safety through the implementation of rigorous process safety management (PSM) systems (Center for Chemical Process Safety, 2007; European Union, 2012; Process Safety Management of Highly Hazardous Chemicals Standard (29 CFR 1910.119), 1992). Process safety focuses on identifying, assessing, and mitigating risks arising from unintentional incidents such as equipment failures, human errors, and operational disruptions, which could lead to catastrophic events, including large hazardous chemical releases, fires, and explosions. (Jain et al., 2017; Kannan et al., 2016). Established methodologies such as Hazard and Operability Studies (HAZOP), Fault Tree Analysis (FTA), and Layer of Protection Analysis (LOPA) have been instrumental in reducing such risks. (Jain et al., 2017; F. Khan et al., 2015). However, while effective, these methodologies often focus on individual hazards and reveal limitations in addressing systemic risks, necessitating more comprehensive frameworks for modern industrial operations (Ab Rahim, Reniers, Yang, et al., 2024; DHS et al., 2014; N. G. Leveson, 2011; H. J. Pasman et al., 2013).

On the other hand, process security focuses on protecting industrial facilities from intentional malicious acts, including sabotage, terrorism, and cyber-attacks (Moorel, 2004; Ta et al., 2020). Despite reports of 373 security-related incidents in industrial facilities (Iaiani et al., 2021), process security has received comparatively less attention than process safety (Ab Rahim, Reniers, Yang, et al., 2024). Established methods, such as the Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF) and Security Vulnerability Assessment (SVA) method, have been developed to address these risks (Matteini et al., 2019; Varadharajan & Bajpai, 2023). However, their application remains underutilized compared to process safety assessments, creating gaps in preparedness for intentional threats (Ab Rahim, Reniers, Yang, et al., 2024; Amin et al., 2022).

Traditionally, process safety and process security have been managed separately, creating silos that result in inefficiencies and gaps in addressing their interconnected risks (Ab Rahim, Reniers, & Yang, 2024; OPCW, 2021; Ylönen et al., 2022). The evolving risk landscape in the CPI—marked by increasing complexity, interconnected systems, and emerging technologies—calls for a more integrated risk management approach that combines both process safety and process security considerations (Ab Rahim, Reniers, Yang, et al., 2024; Ylönen et al., 2022). The growing complexity of CPI operations, driven by technological advancements and dynamic processes, introduces new and unforeseen risks that demand comprehensive strategies (Jain et al., 2017). Nevertheless, current risk management practices often overlook the interdependencies between safety and security risks, reducing the effectiveness of mitigation efforts (Ab Rahim, Reniers, Yang, et al., 2024; Ylönen et al., 2022).

The operations of CPI significantly impact both workers and surrounding communities, making societal values a critical factor in shaping risk management strategies. Societal values refer to the collective convictions that guide decisions in striving for a just and safe society (van de Poel, 2021). Examples include risk reduction, regulatory compliance, operational efficiency, and environmental stewardship (Meyer & Reniers, 2022). These values are central to decision-making processes, as they influence the priorities and trade-offs in managing process safety and process security risks. Aligning these values is essential for creating a cohesive and effective integrated risk management framework, yet the literature offers limited insight into how practitioners perceive and balance these values in practice. Addressing this gap is crucial for understanding the underlying drivers behind integrated risk management decisions in the CPI.

Moreover, resilience engineering has emerged as a promising paradigm to address the gaps in traditional risk management approaches (Aven, 2019; Yang et al., 2023). Resilience engineering emphasizes the ability of systems to anticipate, adapt, and recover from both unintentional and intentional disruptions, including technical failures, terrorism, and natural hazards (H. Pasman et al., 2020b; Yang et al., 2023). Key methodologies, such as the Functional Resonance Analysis Method (FRAM) and System-Theoretic Accident Model and Processes (STAMP), offer a more holistic perspective on risk management by focusing on system-wide interactions and adaptive capacity (Ab Rahim, Reniers, Yang, et al., 2024; H. Pasman

et al., 2020b; Yu et al., 2020). Incorporating resilience principles enables organizations to enhance their ability to manage both process safety and process security risks within a unified framework.

While several studies have highlighted the importance of integrating safety and security risk assessments to improve system resilience (Ab Rahim, Reniers, Yang, et al., 2024; H. Pasman et al., 2020b; Ylönen et al., 2022), there remain significant gaps in empirical research on how practitioners perceive, implement, and adapt to integrated frameworks within the CPI. This study seeks to address these gaps by examining industrial practices, engaging stakeholders in decision-making, gathering insights into practical implementation, and identifying challenges and opportunities for integrating process safety and process security risk management. To achieve this, the following research questions are addressed:

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

This research aims to explore the integration of process safety and process security risk management, leveraging resilience engineering principles to address both unintentional and intentional risks. By assessing the perceptions, awareness, and challenges faced by industrial practitioners, the research identifies critical barriers and enablers while proposing actionable strategies for effective integration. Although the development of a unified framework is beyond the scope of this chapter, the findings provide practitioner-informed insights from the domains of process safety, process security, and resilience engineering. These insights can support industry practitioners in reflecting on integration challenges and provide an empirical basis for the framework development undertaken in Chapter 4.

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

3.2 Methodology

This study adopted a mixed-methods approach, integrating quantitative survey design with qualitative thematic analysis (Stantcheva, 2023; Zairul, 2021; Zou et al., 2014). The primary aim was to explore industry practitioners' perceptions and experiences regarding the integration of process safety and process security risk management. The mixed-methods approach was selected to capture broad trends through quantitative data while also gathering contextual insights via qualitative responses, leveraging the strengths of both methods to support the study's exploratory objectives. However, we acknowledge that survey-based qualitative data collection has inherent limitations, notably less depth and spontaneity. To address this, in-depth interviews with practitioners have been conducted as part of a broader research effort, focusing on follow-up research questions. These interviews will be presented in a separate publication to enrich the understanding of process safety and process security integration.

The survey instrument was developed based on a systematic literature review by the author (Ab Rahim, Reniers, Yang, et al., 2024) and findings by Ylönen et al. (2022) (Ylönen et al., 2022). These studies provided insights into existing practices, challenges, and theoretical frameworks surrounding process safety, process security, and resilience in the CPI. This review informed the formulation of 31 multiple-choice questions designed to assess perceptions and levels of agreement (e.g., Likert scales) alongside six open-ended questions aimed at gathering qualitative insights into barriers, enablers, and strategies for integration.

Before finalizing the survey, a pilot test was conducted with six relevant practitioners and academics, who provided feedback on the clarity, structure, and content of the questions. Their input was incorporated to refine the final version, ensuring that the survey addressed key industry concerns and that respondents could understand the terminology and concepts. The refinements included simplifying definitions, rephrasing ambiguous questions, and restructuring sections for improved flow.

The survey provided definitions of key concepts, including process safety, process security, resilience, and relevant societal values, such as risk reduction and regulatory compliance, to enhance clarity. These definitions were included at the beginning of the related section to ensure that all participants shared a common understanding of the terms, reducing the

risk of misinterpretation. The final survey comprised six sections covering respondent background, current practices, resilience awareness, societal values, barriers, enablers, and strategies for effective integration.

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

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

Qualitative data from the open-ended questions were analyzed using Thematic Analysis Matrix (TAM) model adapted from Zairul (2021). TAM enables the systematic identification and organization of qualitative data through a combination of deductive and inductive coding approaches. Deductive codes are predefined categories based on existing literature or research objectives, such as resilience capabilities. In contrast, inductive

codes are derived directly from the data, representing new or unexpected insights that emerge during analysis.

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

The research team conducted iterative reviews of the codes and themes to ensure accuracy, consistency, and relevance. Qualitative data analysis software, namely ATLAS.ti facilitated transparency and rigor by systematically organizing the data and maintaining traceability to the original responses. These findings were structured and presented using a thematic analysis matrix (e.g., Figure 3 in the Results section), visually illustrating the relationships between codes, categories, and themes.

To ensure transparency and replicability, the survey questionnaire and the anonymized dataset are available through the publicly accessible research repository at: https://data.4tu.nl/datasets/4522882f-0d76-46ad-b63f-5344964e1fb8

The anonymized data is accessible under a CC-BY license, and readers may request additional information from the corresponding author if needed. This study was approved by the Human Research Ethics Committee of TU Delft on 17 January 2024. Participation was voluntary, and no personally identifiable information was collected. The data were anonymized and analyzed in aggregate form to safeguard privacy. Respondents could provide contact details for follow-up interviews, though this was optional.

3.3 Results

3.3.1 Respondent demographics

As shown in Figure **3.1**, a total of 47 participants responded to the survey, representing a diverse range of sectors, positions, and professional experiences within the CPI. The respondents were predominantly based in

Malaysia (61%, n=36) and the Netherlands (23%, n=11), reflecting the survey's outreach and the authors' networks.

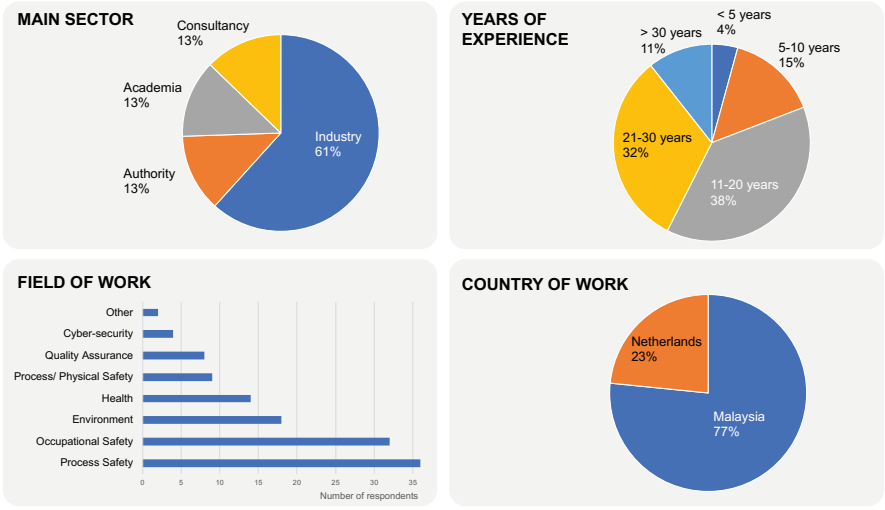

Figure 3.1: Demographic distributions of respondents based on main sectors, years of experience, country of work, and field of work (Adopted from (Ab Rahim, Reniers, & Yang, 2024)

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

The participants brought substantial professional experience to the survey, with 81% (n=38) having over 10 years of experience in their respective fields. Specifically, 38% (n=18) reported between 11-20 years of experience, 32% (n=15) had 21-30 years of experience, and 11% (n=5) had more than 30 years of experience. This high level of expertise among the respondents ensures that the insights gathered from the survey reflect a depth of knowledge in process safety and security risk management practices.

Furthermore, as summarized in Table 1, a cross-tabulation of Country vs. Sector indicates that respondents from Malaysia are predominantly engaged in Industry (58%, n=21), with smaller proportions involved in

Authority (17%, n=6), Consultancy (14%, n=5), and Academia (11%, n=4). Conversely, respondents from the Netherlands were also primarily from Industry (73%, n=8) but with a notable presence in Academia (18%, n=2), while only one respondent reported working in Consultancy.

Table 3.1: The cross-tabulation demographic of respondents is based on country of work, main sectors, and years of experience.

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

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

Regarding Sector vs. Years of Experience, the Industry sector had the most significant representation of respondents with 11-20 years of experience (45%, n=13), followed by those with 21-30 years (24%, n=7). A few participants in Industry had over 30 years of experience (10%, n=3), while some had less than 5 years (3%, n=1). In Academia, most respondents had between 21-30 years (n=3) or more than 30 years of experience (n=1), with very few in the lower experience categories. In Authority, the respondents spread

evenly between five and 30 years of experience, while Consultancy showed concentration distribution across 11 to 30 years of experience ranges.

3.3.2 Perception on integration usefulness

To assess how practitioners perceive the integration of process safety and process security risk management, respondents were asked whether they consider the integration to be useful. **Figure 3.2** provides a visual representation of the perceived usefulness of integration among respondents by country and sector. The graph shows that 72% (n=34) of respondents found the integration useful, 23% (n=11) were neutral, and 4% (n=2) did not find it useful. The left side of the graph illustrates the overall responses, while the flow links to specific countries and sectors on the right side, helping readers understand the breakdown by group.

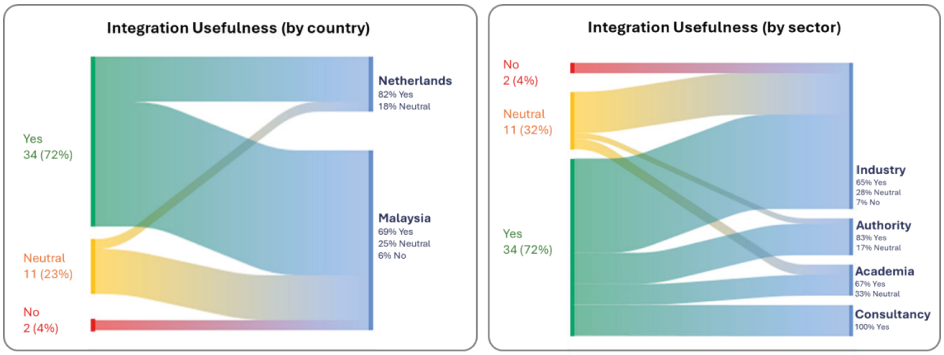

Figure 3.2: Perceived usefulness for the integration among respondents by country and sector.

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

Sectoral analysis revealed further differences. Industry respondents showed strong support, with 66% (n=19) finding integration useful, 28%

(n=8) neutral, and 7% (n=2) not finding it useful. In the Consultancy sector, all respondents (n=6) found integration useful, while in Authority roles, 83% (n=5) found it useful, and 17% (n=1) were neutral. Academia showed a more divided view, with 67% (n=4) finding integration useful and 33% (n=2) expressing neutral opinions.

The qualitative responses provided further depth to these quantitative findings, highlighting why respondents found the integration of process safety and process security useful, as summarized in the Thematic Analysis Matrix (**Figure 3.3**). Several key themes emerged from the open-ended responses, reflecting a consensus on the interconnectedness of safety and security risks and the importance of a proactive, systematic approach to managing them.

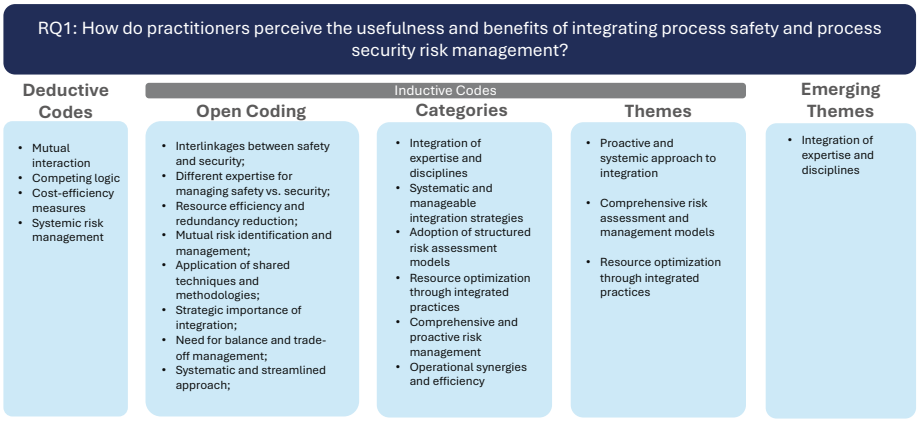

Figure 3.3: Thematic Analysis Matrix on practitioners' perception of the usefulness and benefit of integrating process safety and process security risk management.

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

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

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

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

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

3.3.3 Awareness and perception of the resilience concept

To explore how practitioners perceive the resilience-based approach in managing process safety and security risks, respondents were asked to rate their familiarity with the concept (**Table 3.2**) and their perceptions of its usefulness (**Table 3.3**). The analysis revealed important insights regarding both familiarity and usefulness, as well as how these perceptions vary by country and experience level.

Table 3.2: Familiarity with the resilience concept by country and years of experience.

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

As shown in **Table 3.2**, most respondents (70%, n=33) reported being either slightly or moderately familiar with resilience concepts. In comparison, only a tiny portion (6%, n=3) considered themselves very familiar, and none indicated they were extremely familiar. Familiarity varied notably between countries and across different levels of professional experience. Among Malaysian respondents, familiarity levels were more diverse, particularly within the 11-20 years of experience group, where responses ranged from not at all familiar to very familiar. In contrast, Dutch respondents with more than 21 years of experience mostly (91%) described themselves as slightly or moderately familiar, with none reporting very or extremely familiar. These findings suggest that while moderate familiarity is common, a more profound understanding of resilience concepts is limited, particularly in the Netherlands, where even highly experienced practitioners tend to lack advanced familiarity.

Table 3.3: Perceived usefulness of resilience concepts by country and years of experience.

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

In terms of perceived usefulness (**Table 3.3**), the majority of respondents (45%, n=21) found resilience concepts to be useful, while 13% (n=6) considered them very useful. Notably, there was variation in how practitioners from different countries and experience levels rated the usefulness of resilience concepts. Among Malaysian respondents, 16 out of 36 participants (61%) rated resilience as either useful or very useful, indicating more substantial overall support for resilience-based approaches. In contrast, among Dutch respondents, only 5 out of 11 participants (45%) rated resilience concepts as either useful or very useful, reflecting a more mixed perception.

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

Furthermore, the heatmap analysis in **Figure 3.4** provided additional insights into the relationship between familiarity and perceived usefulness. Respondents who were moderately familiar with resilience concepts were the most likely to find them useful or very useful, whereas those with only slight familiarity tended to remain neutral. This suggests that moderate familiarity is sufficient for practitioners to recognize the value of resilience-based approaches. However, the lack of respondents in the "extremely familiar" category and the relatively high number of neutral responses across all familiarity levels indicate that deeper understanding or practical exposure may be needed to appreciate the benefits of resilience-based approaches fully.

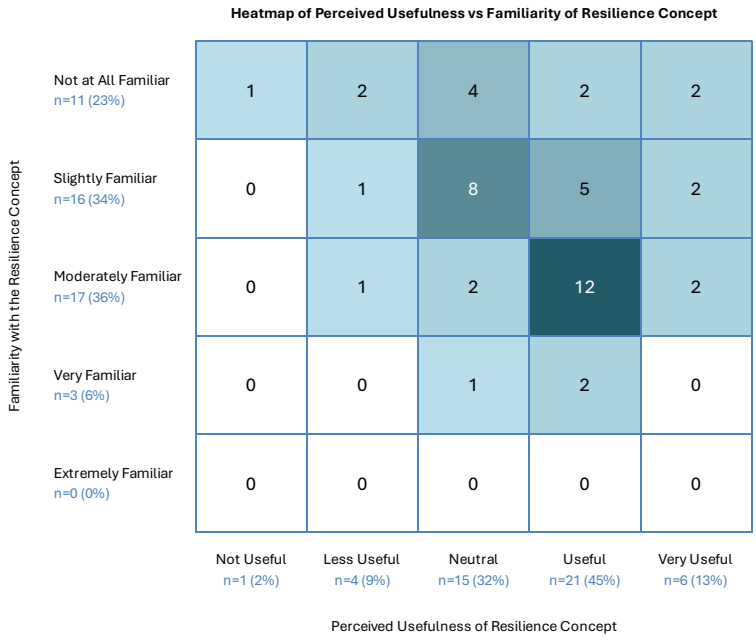

Figure 3.4: Heatmap of perceived usefulness vs. familiarity on resilience concept among respondents.

We also ask the respondent in an open-ended question to list any resilience-based practices or principles they are aware of. The qualitative responses supported these quantitative findings, revealing several key categories and themes that align with broader resilience frameworks (**Figure 3.5**). One key category that emerged was anticipation and proactivity. Respondents emphasized the importance of anticipating risks

and taking proactive measures to mitigate them before they escalate. For instance, a consultant from Malaysia highlighted anticipation as a key practice in resilience, stressing the need for early identification of potential threats. This reflects the proactive stance central to resilience-based approaches, which aim to address risks before they become critical issues.

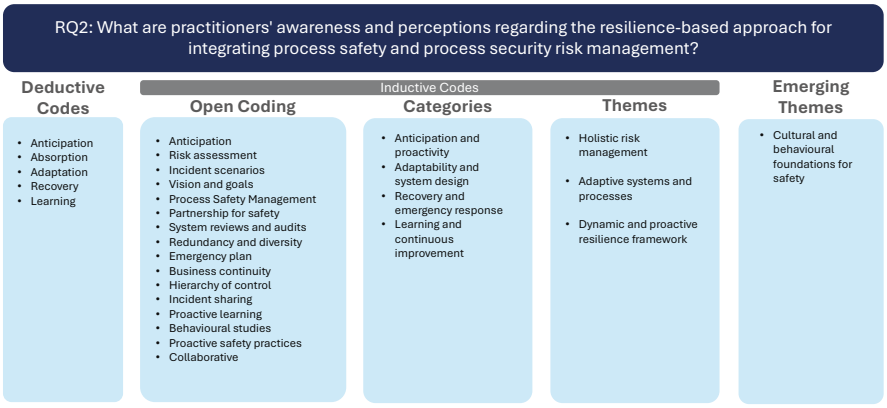

Figure 3.5: Thematic Analysis Matrix on practitioners' awareness and perception of the resilience-based approach for integrating process safety and process security risk management.

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

Respondents also mentioned the categories of recovery and emergency response. Respondents emphasized the importance of having effective recovery and emergency response mechanisms in place to ensure that operations can continue or recover quickly in the event of an incident. A consultant from Malaysia pointed to business contingency plans as a key resilience practice that allows organizations to bounce back from

disruptions. This category also includes practices like emergency response planning and incident sharing, which enable organizations to learn from incidents and enhance their resilience over time.

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

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

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

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

Lastly, the cultural and behavioral foundations theme highlights that resilience is supported by organizational leadership, teamwork, and a proactive safety culture. This theme emerged from the category focused on organizational culture, where respondents recognized that resilience is not only about systems but also about the people who operate within those systems. Leadership, collaboration, and a commitment to proactive safety behaviors are seen as critical components of a resilient organization, reinforcing the idea that resilience is as much about people and culture as it is about technical systems.

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

3.3.4 Importance of different societal values

In industrial settings, professionals frequently face challenging decisions that involve balancing the sometimes-conflicting values of process safety and process security. This section examines how practitioners prioritize these values across five hypothetical risk scenarios, each presenting a trade-off between process safety and process security (**Figure 3.6**). The scenarios are briefly mentioned below, and full descriptions can be found in **Appendix B**.

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

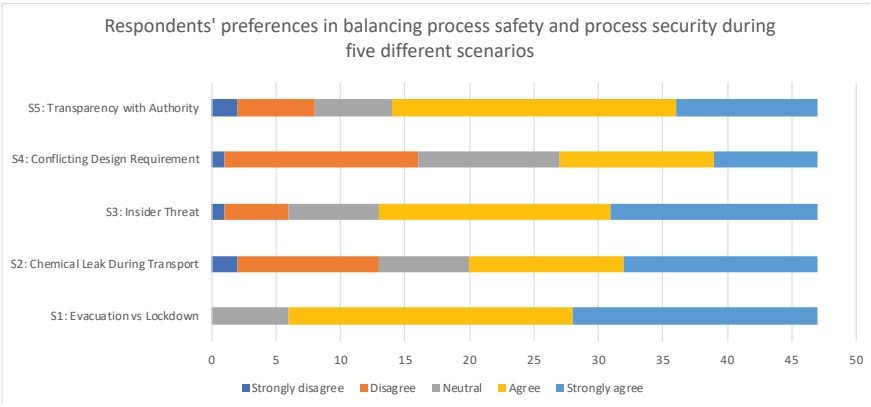

Figure 3.6: Respondents' preferences in balancing process safety and process security during five different scenarios.

In Scenario 2 (Chemical leak during transport), respondents considered whether to immediately inform the public about a chemical leak, prioritize safety, or secure the transport from potential threats before making any disclosures. A majority (57%) supported prioritizing public safety, but a notable proportion (28%) disagreed, showing concern for securing hazardous materials first. This finding illustrates the complexity of balancing safety with security in scenarios involving hazardous substances.

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

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

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

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

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

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

The results from Scenario 5 also suggest that while process security is important, regulatory compliance and safety-driven transparency take precedence. The tension between safety and security underscores the

need for integrated frameworks that balance safety and security without compromising one for the other. Practitioners could benefit from tools and approaches that help them make informed decisions when process safety and process security come into conflict, ensuring that neither aspect is neglected in critical situations.

In addition to evaluating specific safety and security scenarios, respondents were asked to rank various societal values based on their importance in process safety and process security contexts (Meyer & Reniers, 2022). The ranking, shown in **Table 3.4**, highlights key priorities in both domains and reveals some significant differences.

Table 3.4: Respondent's ranking of societal values in process safety and process security risk management.

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

The two highest-ranked values across both process safety and process security were Risk reduction potential and Risk creation, but their order differs between the two domains. In process safety, risk reduction potential emerged as the top priority, indicating that practitioners prioritize actions that can prevent incidents and reduce losses. This reflects the core objective of process safety: minimizing harm and preventing accidents. Conversely, in process security, risk creation was ranked as the most important value, emphasizing that practitioners are more concerned with preventing the introduction of new risks or vulnerabilities, especially those related to malicious actions, such as theft or sabotage. This difference highlights the distinction between unintentional risks in safety and intentional risks

in security. The focus on minimizing new risks in security suggests that the primary goal is not just to reduce existing risks but also to prevent any additional threats from emerging.

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

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

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

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

Values such as equity, fairness, and administrative efficiency were ranked lower in both process safety and process security. Fairness ranked last in both domains, indicating that concerns about the fair distribution of costs

or responsibilities are often secondary to more immediate considerations such as risk reduction or cost-effectiveness.

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

In summary, the ranking, shown in **Table 3.4**, highlights key priorities in both domains and reveals some important differences. These differences highlight the need for integrated risk management frameworks that can accommodate these varying priorities. Practitioners should balance economic, environmental, and regulatory concerns while addressing both intentional security risks and unintentional safety risks. In conclusion, while many values are shared between process safety and process security, differences in prioritization suggest that a holistic approach is needed to manage risks effectively in both domains.

3.3.5 Barriers and enablers for integration

In the survey, practitioners were asked to rank the main barriers to integrating process safety and process security risk management (Ylönen et al., 2022). Lack of knowledge and awareness emerged as the most significant barrier (**Figure 3.7**). This highlights that many practitioners still lack a foundational understanding of how to effectively integrate safety and security processes, which represents a critical obstacle.

The second-highest barrier was insufficient resources such as time, budget, and personnel. This may indicate that organizations struggle with resource constraints, which limit their ability to implement comprehensive integration strategies. For instance, budgetary limitations may prevent cross-disciplinary training, while time pressures may lead to short-term measures over integrated, long-term solutions. Lack of willingness and communication between safety and security teams emerged as the third major barrier. Respondents cited in an open-ended response that poor communication and organizational silos as key challenges that prevent safety and security professionals from collaborating effectively. Regulatory challenges and inadequate technology solutions were ranked lower but

remained relevant. Unclear or conflicting regulatory requirements and the need for better technological tools were noted by respondents, who emphasized the importance of aligning regulatory frameworks to support integration.

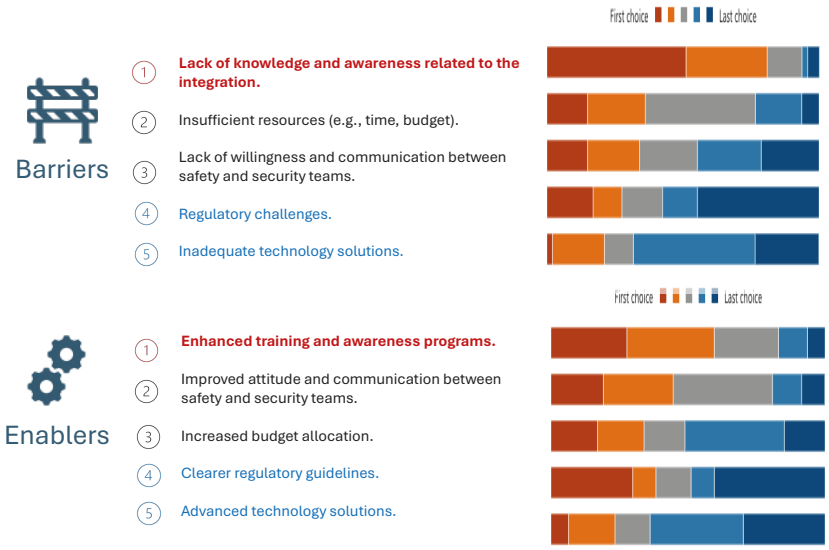

Figure 3.7. Respondents' preferences in balancing process safety and process security during high-risk scenarios.

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

The qualitative analysis revealed key themes that further illuminate the complexity of integrating process safety and security (**Figure 3.8**).

The intertwined nature of barriers was a prominent theme, where respondents identified a mix of organizational, technical, and regulatory challenges. For instance, a respondent from Malaysia noted the "*lack of communication and commitment*" between departments, while a respondent from the Netherlands highlighted inadequate regulatory enforcement as a barrier.

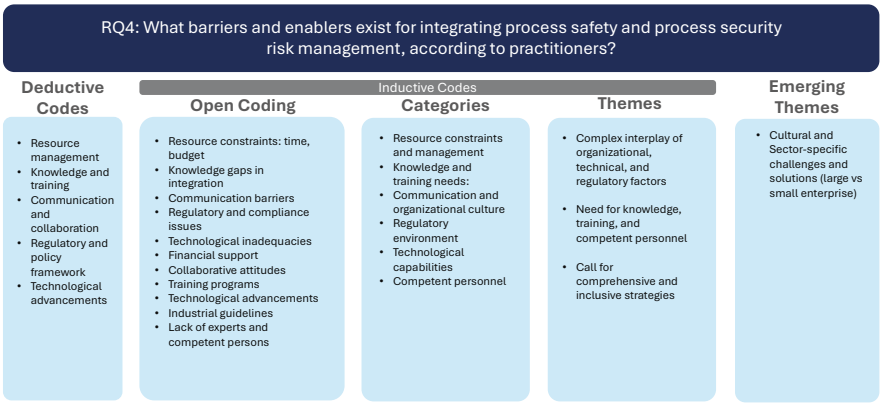

Figure 3.8. Thematic Analysis Matrix on barriers and enablers for integrating process safety and process security risk management.

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

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

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

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

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

3.3.6 Proposed strategies for integrating process safety and process security

Respondents were asked to rate six proposed strategies for integrating process safety and security risk management (Ab Rahim, Reniers, Yang, et al., 2024; Ylönen et al., 2022). These strategies included developing joint policies, conducting integrated risk assessments, and fostering clear communication channels. The quantitative data (**Figure 3.9**) provided insights into the perceived effectiveness of these strategies, with notable

differences in ratings between respondents from Malaysia and the Netherlands.

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

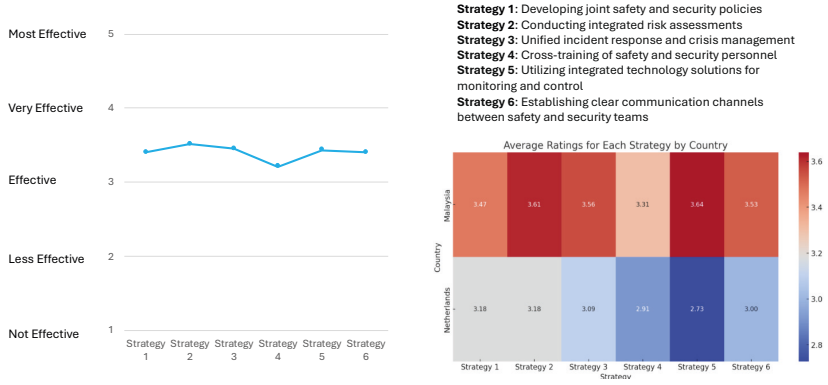

Figure 3.9. Respondent's rating on the effectiveness across six integration strategies.

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

However, strategies like cross-training safety and security personnel (3.21 overall) and utilizing integrated technology solutions (3.42 overall) received lower ratings, especially from Dutch respondents. These differences suggest regional or organizational variations in the perceived feasibility of such measures, with Malaysian respondents being more favorable toward the use of technology and cross-training.

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

Thematic analysis of open-ended responses revealed deeper insights into these strategies (**Figure 3.10**). Resilience-oriented risk management emerged as a key theme, with respondents emphasizing the need for proactive, adaptive strategies that balance safety and security. While not always explicitly rated as a standalone strategy, several respondents indirectly supported resilience principles through their emphasis on holistic risk and crisis management. One respondent suggested the creation of "*specific expert teams*" to focus on integrated risk assessments, while another stressed the importance of having clear guidelines for managing safety and security during crises. This highlights the importance of having a well-defined crisis management plan that integrates both safety and security considerations and supports resilience by ensuring that core functions are maintained even in the face of disruption.

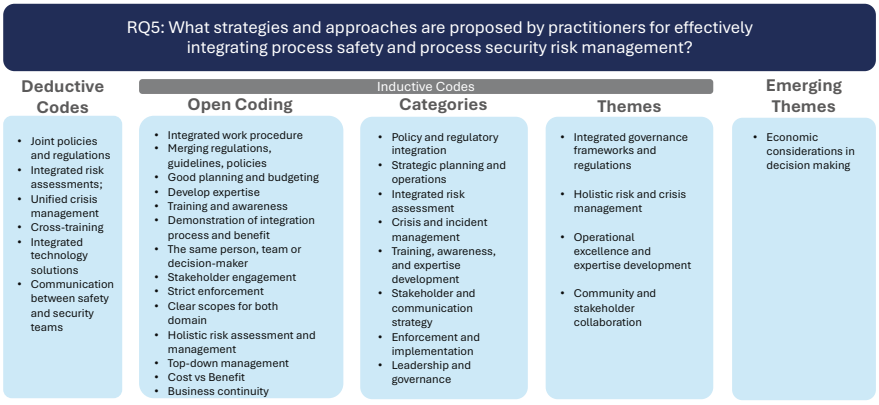

Figure 3.10: Thematic Analysis Matrix on strategies and approaches for integrating process safety and process security risk management.

Respondents also highlighted the need for integrated governance frameworks. Several called for "*merging regulations or guidelines*" to support alignment between safety and security. The role of top

management was frequently mentioned, with one respondent noting that "*top management or the executor for safety and security should be the same person*," stressing the need for unified leadership.

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

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

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

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

3.4 Discussions

3.4.1 Interpretation of findings

3.4.1.1 Integrating process safety and process security risk management

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

One respondent (Malaysian authority personnel) noted, "*In most cases, safety and security risks share the same hazard and effect. The differences would be in terms of intention (intentional vs. unintentional).*" This perspective aligns with the growing body of literature that emphasizes the convergence of safety and security in high-risk industries, where integrating both domains is key to improving risk management outcomes (Ab Rahim, Reniers, Yang, et al., 2024; El-Kady et al., 2023; Pettersen Gould & Bieder, 2020a). Studies have shown that integrated frameworks reduce redundancies, enhance efficiency, and improve overall risk management outcomes (Amin et al., 2022; Bischoff et al., 2015; Kriaa et al., 2015; Ylönen et al., 2022). However, achieving integration remains challenging due to organizational silos and differing priorities between safety and security teams remain significant barriers to attaining integration (Ab Rahim, Reniers, & Yang, 2024; Baybutt, 2017b; Pettersen Gould & Bieder, 2020a).

The findings also suggest that integration is a foundational element of resilience in chemical process industries, as it ensures comprehensive coverage of both unintentional and intentional risks (Aven, 2019; Jain, Mentzer, et al., 2018b; Yang et al., 2023). Practical approaches to integration, as evidenced by the survey results (Figure 9), may include joint risk assessments and shared training programs for safety and security personnel. These strategies could enhance communication and collaboration, ultimately fostering more cohesive and resilient operations. For example, joint training sessions and drills could focus on scenarios incorporating both process safety and process security, encouraging cross-disciplinary understanding and teamwork.

3.4.1.2 Awareness and usefulness of resilience-oriented approaches

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

One respondent illustrated this by stating, *"Proactive learning from successful task or event* ". This statement reflects a core principle of resilience engineering: learning from both successes and failures to improve system robustness and adaptability (Aven, 2017; Hollnagel, 2006; Jain, Pasman, et al., 2018a). As the literature highlights, such proactive learning is essential for enhancing process and organizational resilience in the face of disruptions (Jain, Rogers, et al., 2018e; Yarveisy et al., 2022).

However, the survey also highlighted variations in familiarity levels, which may reflect differences in organizational focus, roles, or geographic contexts. These variations underscore the need for education and training initiatives to increase awareness and understanding of resilience principles across the chemical process industry. As noted by Patriarca et al. (2018) (Patriarca, Bergström, et al., 2018), targeted training can enhance stakeholders' capacity to anticipate and adapt to emerging risks, particularly in complex and dynamic environments. Similarly, Woods (2015) (Woods, 2015) emphasizes that scenario-based training is effective in fostering a shared understanding of adaptability and proactive risk management among multidisciplinary teams. The findings suggest practical strategies for leveraging resilience-based approaches, such as incorporating resilience principles into existing risk management frameworks or using scenario-based training to highlight adaptability and proactive risk identification. Addressing barriers, such as lack of familiarity or organizational inertia, will be critical to realizing the full potential of resilience engineering in practice (Jahangiri et al., 2021; Yang et al., 2023).

3.4.1.3 Importance of societal values in risk management

Both the quantitative and qualitative data highlight the importance of aligning societal and organizational values—such as risk reduction, regulatory compliance, and operational efficiency—in supporting integrated risk management. This echoes findings in risk management literature, where value alignment is seen as critical for creating a cohesive decision-making environment in a dynamic socio-technical system (Meyer & Reniers, 2022; Rasmussen, 1997a). Among respondents, one of the most consistently prioritized values was "Risk reduction potential," which ranked highly in both process safety and process security domains, demonstrating that shared values can minimize conflicts between safety and security objectives (Kriaa et al., 2015; G. Reniers et al., 2020). Focusing on shared values helps organizations create environments where process safety and process security objectives are mutually reinforcing rather than competitive (Ylönen et al., 2022). This alignment facilitates the development of integrated risk management frameworks that prioritize safety, security, resilience, and business continuity (Ab Rahim, Reniers, Yang, et al., 2024; Jain et al., 2020).

However, aligning values in practice can be complex, mainly when trade-offs are necessary between competing objectives. For instance, regulatory compliance may sometimes emphasize security measures that inadvertently increase operational risks. Organizations can address these challenges through structured workshops and stakeholder consultations, prioritizing shared goals and mutual understanding (Jayaraman et al., 2020; Ktori et al., 2024). Incorporating societal values into organizational policies and decision-making frameworks can further strengthen alignment, as suggested by De Bruijn and Herder (2009) (de Bruijn & Herder, 2009). These strategies enable organizations to create integrated risk management systems adaptable to evolving societal expectations and operational demands.

3.4.1.4 Barriers and enablers for integration

The survey identified several barriers to effective integration of process safety and security risk management, mirroring findings from previous studies on integration practices (Ylönen et al., 2022). The most highly ranked barriers included a lack of knowledge and awareness, insufficient resources, and communication challenges between safety and security teams. For example, an academician from Malaysia noted, "*Creating*

awareness at all levels on the significance for integrating process safety and process security risk management." These findings emphasize the need for enhanced training programs to build cross-disciplinary awareness and expertise, increased budget allocations to support integration efforts, and improved communication channels to foster collaboration.

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

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

3.4.1.5 Effective strategies for integration

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

Additionally, the emphasis on cross-training personnel points to the importance of equipping professionals with the skills and knowledge necessary to simultaneously manage both process safety and process security risks. Research highlights that training programs designed to build interdisciplinary skills can improve communication and foster mutual understanding across different domains (Ab Rahim, Reniers, & Yang, 2024; Ylönen et al., 2022). Such training ensures that safety and security teams can collaborate effectively, leveraging shared knowledge to address overlapping risks (Fouzi et al., 2024; N. G. Leveson & Stephanopoulos, 2014).

To ensure the success of these strategies, organizations must implement robust performance indicators to monitor progress and evaluate the effectiveness of integration efforts (Jovanović et al., 2018; F. Khan et al., 2010; H. Pasman & Rogers, 2014). Reniers et al. (2011) (G. Reniers et al., 2011) suggest that performance indicators should encompass management, process, and result dimensions to provide a holistic view of risk management practices. For instance, metrics such as leadership commitment, the frequency of integrated risk assessments, and reductions in incident response times can offer actionable insights into areas requiring improvement. These indicators guide continuous improvement efforts and provide measurable evidence of integration success.

However, implementing these strategies requires addressing potential barriers, such as resource constraints, organizational inertia, and the need for cultural change (Jahangiri et al., 2021; OPCW, 2021; G. Reniers et al., 2011). For example, while joint policies and integrated tools can improve alignment, their adoption often requires significant investment and management buy-in. Practical approaches to overcome these challenges include establishing leadership roles dedicated to integration, securing funding through cost-benefit analyses, and promoting pilot programs to demonstrate the effectiveness of integrated strategies (G. Reniers et al., 2011).

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

3.4.2 Synthesis of the grand themes

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

3.4.2.1 Theme 1: Proactive and systemic approach to risk management

A proactive and systemic approach to risk management emerged as a central theme across the responses. This theme aligns with the literature on integrated risk management, which highlights the necessity of addressing interdependent risks in a unified framework (Logan et al., 2022; G. Reniers et al., 2011; Ta et al., 2020). Respondents emphasized the interconnected nature of safety and security risks and advocated for a structured and proactive strategy to manage these risks. This approach involves mutual risk identification, resource optimization, and the strategic integration of expertise. Many respondents highlighted the benefits of adopting a more holistic view, where process safety and security are not treated as isolated silos but as interdependent components of a comprehensive risk management framework. (N. G. Leveson & Stephanopoulos, 2014) argued that a systemic approach to risk management can streamline operations and create a more resilient process system.

3.4.2.2 Theme 2: Resilience-oriented systems and processes

Resilience was another dominant theme, with respondents underlined the importance of adaptability, emergency response, and business continuity. Resilience-based approaches focus on proactive measures, including anticipation and rapid recovery from disruptions, consistent with resilience engineering frameworks (Cheng et al., 2022; Jain, Pasman, et al., 2018a; Yarveisy et al., 2020). Resilience enables organizations to absorb and recover from both unintentional and malicious threats, particularly in a complex engineered system such as CPI (Logan et al., 2022; Yang et al., 2023). One respondent noted a resilience-oriented approach, "*Proactive learning from successful task or event*", reflecting key principles from resilience literature. The focus on anticipation and continuous improvement aligns

with the "adaptive capacity" concept in resilience theory, which is critical for managing risks in dynamic environments (H. Pasman et al., 2020b).

3.4.2.3 Theme 3: Strategic alignment of societal values

The strategic alignment of values was also identified as a crucial factor for successful integration. Respondents stressed the need to align societal values, such as risk reduction, regulatory compliance, and operational efficiency, to support integrated risk management. This alignment is essential for minimizing conflicts and enhancing decision-making processes (Amundrud et al., 2017; G. Reniers et al., 2020). By aligning values across process safety and process security domains, organizations can create a more cohesive and effective risk management strategy (Ylönen et al., 2022).

3.4.2.4 Theme 4: Leadership, governance, and collaboration

Effective leadership, governance, and collaboration emerged as one of the key enablers for integrating process safety and security risk management. Respondents identified strong leadership and governance structures that support cross-functional collaboration as vital for fostering system resilience. The importance of clear communication channels and collaborative efforts between process safety and security teams was frequently mentioned. As noted by one respondent, "*Top management or executer for safety and security operations and measures are same person"*, could be an effective strategy. Similar to the literature, this study also suggested that organizational leadership should actively promote and support integration efforts to ensure their success (G. Reniers et al., 2011; G. L. L. Reniers, 2010).

3.4.2.5 Theme 5: Continuous improvement and adaptation

The theme of continuous improvement and adaptation was prominent in the qualitative responses, aligning with literature on adaptive risk management and organizational learning (Kriaa et al., 2015; Meyer & Reniers, 2022; Rasmussen, 1997a). Respondents highlighted the need for ongoing learning and adaptation, leveraging new technologies and data analytics to enhance system resilience. Proactive learning, system reviews, and integrating behavioral studies into risk management practices were critical for maintaining and improving resilience. Respondents advocated for a dynamic approach to risk management that evolves with changing conditions and emerging threats.

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

3.4.3 Recommendations

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

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

Secondly, organizations should consider the use performance indicators to monitor and evaluate progress toward resilience-oriented integration of process safety and security risk management (N. Leveson, 2015). Respondents highlighted the importance of clear metrics to ensure continuous progress in integrating safety and security practices. Building on Reniers et al. (2011) (G. Reniers et al., 2011), these indicators could cover management, process, and result dimensions, providing a basis for examining how integration is functioning in practice. Management indicators might focus on leadership commitment, resource allocation,

and cross-functional collaboration. Process indicators could assess the frequency and quality of integrated risk assessments, cross-training initiatives, and the adoption of advanced technologies. Result indicators might measure incident response times, reductions in risk exposure, and overall system resilience. By regularly tracking these performance indicators, organizations can identify areas for improvement and support continuous progress in strengthening both safety and security efforts.

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

Furthermore, ongoing investment in continuous improvement and advanced technology, such as real-time monitoring and data analytics, is critical for enhancing risk management. Emerging technologies such as digital twins and machine learning (ML) offer additional opportunities for improving risk management. Digital twins can simulate process scenarios, enabling proactive identification of vulnerabilities and testing of integrated safety-security strategies(Alsulieman et al., 2024; Bevilacqua et al., 2020) ML algorithms can enhance predictive capabilities, detecting patterns in operational data to anticipate risks and optimize mitigation efforts (Raveendran et al., 2022). Leveraging these tools enables data-driven assessments and strengthens system resilience.

Finally, leadership plays a pivotal role in promoting integration efforts. Senior management should allocate necessary resources, foster a culture of collaboration, and establish dedicated roles to oversee integration initiatives (G. Reniers et al., 2011). Leaders should also encourage collaboration between safety and security teams through joint training programs and clear communication channels (Ab Rahim, Reniers, & Yang, 2024). Pilot programs and phased implementation of strategies

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

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

3.5 Conclusions

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

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

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

Though this research provides valuable insights, several limitations must be acknowledged. The sample size limits the generalizability of findings, and reliance on self-reported data introduces potential biases. Future research could address these limitations by expanding the scope to other high-risk sectors, such as healthcare, transportation, and energy, and by employing longitudinal designs to assess the long-term effectiveness of integration efforts. Additionally, in-depth qualitative methods, such as interviews and case studies, could provide richer narratives and deeper insights into organizational dynamics and practical applications of integration strategies. The role of advanced technologies in supporting integration is another promising avenue for future research. Exploring the adoption and impact of real-time monitoring, data analytics, and AI-driven tools across industries could provide critical insights for developing more sophisticated integrated frameworks.

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

Chapter 4



Developing the RoPSS Framework: A Resilience-oriented Approach to Integrated Process Safety and Process Security Risk Management

Chapter 3 showed that practitioners generally recognize the value of integrating process safety and process security risk management, but also identified important barriers, including knowledge gaps, resource constraints, communication silos, and limited familiarity with resilience-oriented thinking. These findings indicate that integration requires more than conceptual agreement; it requires a structured framework that can translate resilience engineering into practical management logic. Chapter 4 addresses this need by developing the Resilience-oriented Process Safety and Process Security (RoPSS) framework, which organizes integrated risk management around four resilience capabilities, eight disruption types, and a performance indicator architecture.

This chapter is written with modifications based on the following research article: Ab Rahim, M. S., Reniers, G., & Yang, M. (2026). A resilience-oriented framework for managing process safety and process security. Process Safety and Environmental Protection, 215, 109182. https://doi.org/10.1016/j.psep.2026.109182

ABSTRACT

This chapter develops the Resilience-oriented Process Safety and Process Security (RoPSS) framework, which integrates process safety and process security through four resilience capabilities: Anticipation, Absorption, Adaptation, and Ascension. 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. The RoPSS framework addresses this challenge by embedding the four resilience capabilities 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.

4. DEVELOPING THE ROPSS FRAMEWORK

4.1 Introduction

The chemical process industry (CPI) operates under inherently high-risk conditions 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 (Directive 2012/18/EU, 2012; 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 & 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, Reniers, Yang, 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 (G. 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 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 & 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 & Bjørnskau, 2015; G. 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 & 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 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; H. Pasman et al., 2020b). 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; H. Pasman & 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 governance structures that enable cross-boundary learning 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 & Bieder, 2020a; G. 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 **Figure 4.1.**

This chapter addresses these gaps by developing the Resilience-oriented Process Safety and Process Security (RoPSS) framework as an expert-informed conceptual framework designed for operationalization. The chapter 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.

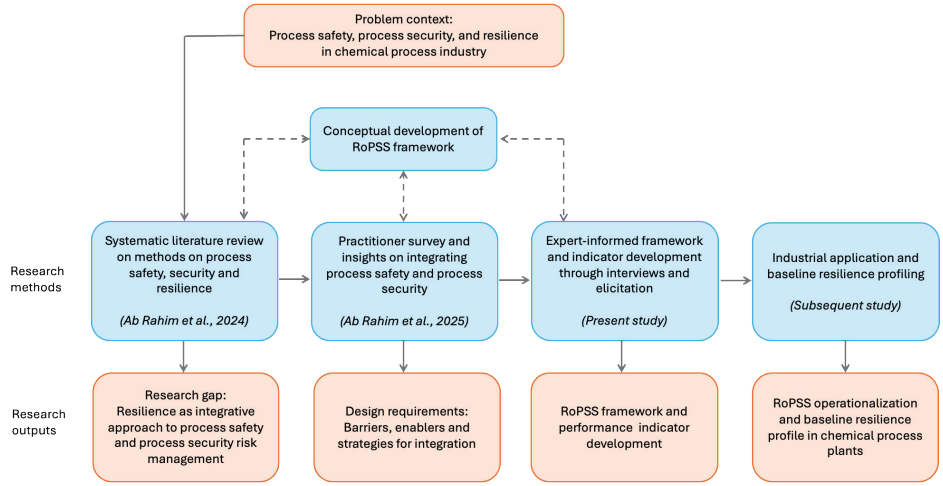

Figure 4.1: Research roadmap showing the development of the RoPSS framework within the broader research program.

The remainder of this chapter is organized as follows. Section 2 presents the conceptual foundations of unified risk management, coupled safety–security dynamics, resilience capabilities, governance resilience, 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.

4.2 Conceptual and theoretical construct

4.2.1 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 (H. Pasman et al., 2020b; Rasmussen, 1997b). 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. 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, Reniers, Yang, 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., 2016b; 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 resilience perspective acknowledges the emergent and non-linear nature of socio-technical performance variability (Ab Rahim, Reniers, Yang, 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, Khakzad, & Reniers, 2020; Yuan et al., 2024; F. 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, Rogers, et al., 2018c; H. Pasman et al., 2020b). 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 & Trump, 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.

4.2.2 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 & 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 & Gould, 2020; N. Leveson, 2020).

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 & 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 (F. 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, Bergström, 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 percent 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 & Reniers, 2020; Schulman, 2020). Managing such coupling, therefore, requires organizational capabilities that maintain functional balance and adaptability without undermining either domain.

4.2.3 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 & 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, Bergström, 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., 2020a; Yarveisy et al., 2022).

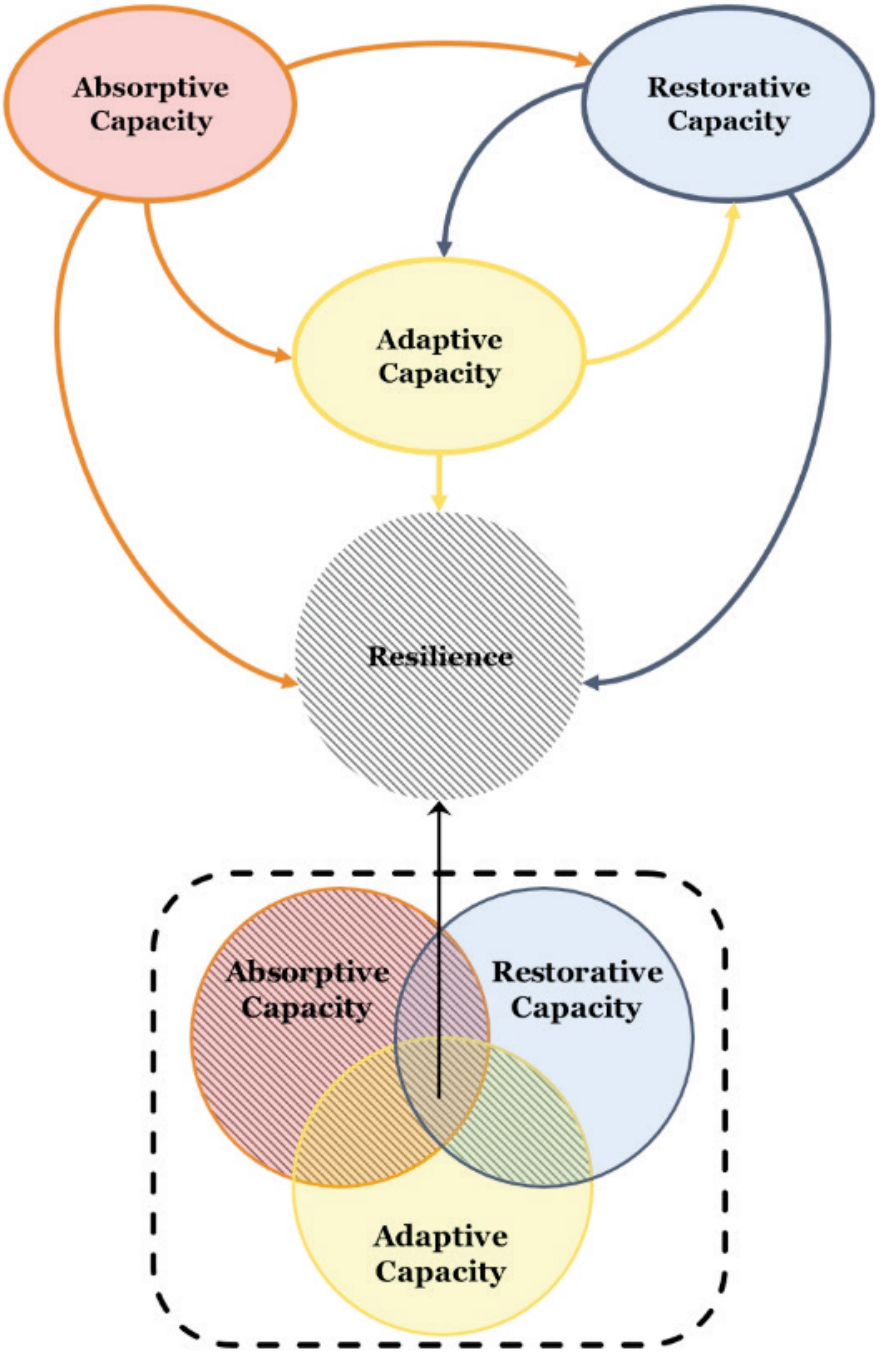

Figure 4.2: Logical relation of system capacities with resilience (adopted from Yarveisy et al., 2020).

Yarveisy et al. (2020) conceptualized these interrelations through absorptive, adaptive, and restorative capacities **(Figure 4.2**). 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, Bergström, 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 process safety and process security. Through this capability, resilience becomes progressive rather than merely cyclical, characterized by continuous refinement of functions, coordination, and foresight.

4.2.4 From operational to governance resilience

While the four resilience capabilities describe how systems anticipate, absorb, adapt, and ascend before, during, and after disruption, much resilience engineering research has focused on operational aspects such as control room performance, barrier reliability, or procedural response (Jain, Diangelakis, et al., 2019; Sun, Yang, et al., 2022; Zeng et al., 2025). Yet the persistence and evolution of resilience in the CPI also depend on governance, namely the leadership, organizational structures, and policy environments that shape how learning, investment, and cross-functional coordination are sustained over time (H. Pasman et al., 2020b; Zio, 2018).

Operational resilience concerns how frontline systems behave under pressure, including detecting early warnings, maintaining containment, restoring production, and protecting people and assets. These functions

are largely technical and procedural, embedded in the plant's maintenance, management of change, and emergency response systems (Hosseini et al., 2016b; Mentges et al., 2023). Governance resilience, by contrast, concerns the institutional capacity to create and sustain the conditions that make operational resilience possible. It encompasses leadership commitment, resource allocation, regulatory alignment, organizational learning, and strategic foresight (Hansen & Antonsen, 2024; Hollnagel, 2006). Consistent with the OECD *Good Governance for Critical Infrastructure Resilience* (OECD, 2019), governance resilience requires coherent policy frameworks, cross-sector coordination, and mechanisms for institutional learning that ensure operational insights can be translated into long-term improvements.

This vertical scaling of resilience implies that Ascension capability, must operate not only at the technical and procedural levels but also through management systems, policy instruments, and inter-organizational collaboration. Leadership behaviors such as transparent communication, just culture, and system-wide learning programs become enablers of Ascension at the governance level, allowing lessons from one facility or domain to strengthen the broader safety–security system. In practice, resilience is sustained through learning loops that connect operational signals to governance responses (Pettersen & Bjørnskau, 2015; Schulman, 2020). The OECD *Guiding Principles for Chemical Accident Prevention, Preparedness and Response* (OECD, 2023) emphasize this continuum, highlighting the importance of strategic foresight, horizon scanning, and continual regulatory refinement, including anticipating future risk conditions, monitoring weak signals and emerging trends, and updating governance arrangements in light of new lessons and changing contexts.

Despite this need for integrated learning loops, many organizations continue to face barriers that fragment operational and governance functions. Insights from the practitioner survey reported in (Ab Rahim et al., 2025) revealed that practitioners often perceive limited integration between site-level safety and corporate security management, citing siloed policies, unclear leadership ownership, and insufficient follow-up after incidents. These gaps suggest that resilience cannot be sustained solely through operational performance; it also requires governance structures that promote shared accountability, long-term orientation, and continuous improvement (OECD,2023).

Within the proposed framework, governance mechanisms are embedded within each resilience capability. At the governance level, Anticipation involves strategic foresight, horizon scanning, and policy development that recognize systemic interdependencies in safety and security. Absorption includes maintaining resource redundancy, budget contingencies, and organizational capacity to withstand regulatory, market, and operational shocks. Adaptation reflects the agility of management systems to adjust priorities, delegate authority, and realign decision structures during crises. Ascension translates lessons from disruptions into institutional reforms such as revised standards, updated procedures, leadership development, and inter-agency cooperation that enhance both safety and security governance.



Through this multi-level integration, the framework conceptualizes resilience not merely as a property of engineered systems but as a governance function that spans organizational hierarchies and stakeholder boundaries. Resilience, therefore, depends on alignment between operational responses and the governance structures that shape long-term learning, resource allocation, and cross-domain coordination.

4.2.5 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 (F. Khan et al., 2010). Existing systems also tend to prioritize lagging outcomes and monitor safety and security through separate metrics and reporting channels (G. 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 offers a practical pathway for operationalizing integration between process safety and process security within a unified resilience-oriented framework (Ab Rahim et al., 2025; N. Leveson, 2015; H. Pasman & Rogers, 2014; Yarveisy et al., 2022).

Resilience measurement should 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 (H. Pasman & Rogers, 2014). Recent research highlights indicator- and index-based approaches as useful semi-quantitative tools when probabilistic data are limited (Hosseini et al., 2016b; 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; F. 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 (N. 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).

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, ensuring that performance measurement reflects both technical robustness and organizational learning. Unlike conventional leading–lagging systems that 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 also addressing both safety and security concerns. (Meyer & Reniers, 2022). When designed accordingly, they provide a balanced picture of system resilience, capturing management intent, operational performance, and learning outcomes. They also serve as decision-support instruments that guide resource allocation and strategic prioritization.

Importantly, these indicators link operational and governance resilience. At the operational level, they track system performance and adaptive behavior. At the governance level, they measure leadership commitment,

institutional learning, and embedding resilience principles into organizational policies and standards. This dual function ensures coherence between what is measured at the plant level and what is managed at the organizational and regulatory levels.

Aligned with established international guidance and grounded in the four resilience capabilities, the indicator typology developed in this study provides a structured means of linking resilience concepts with practical implementation. In this sense, indicators act as measurable connectors between risk management, operational control, and governance learning. They help translate resilience into an actionable, continuous process of system improvement.

4.2.6 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. (N. 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 (**Figure 4.3)**. 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.

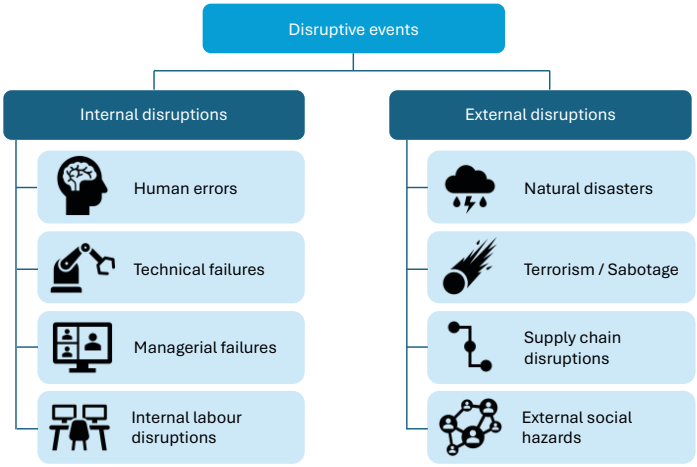

Figure 4.3: Classification of disruptive events encompasses eight disruption types (four internal and four external)

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.

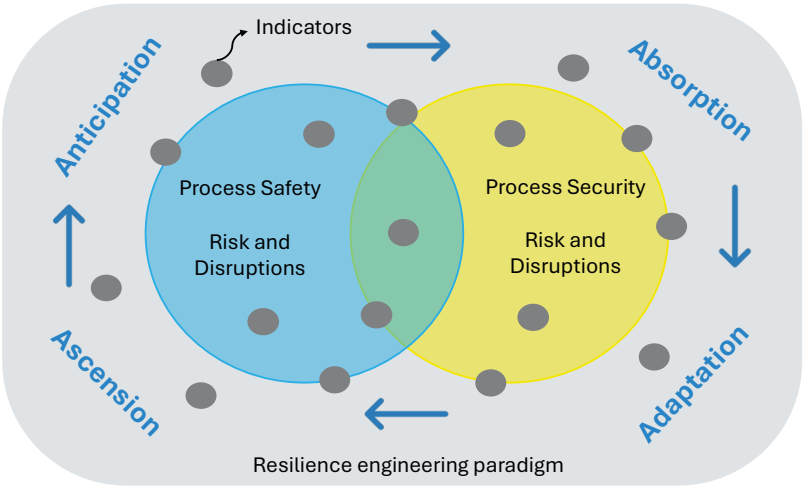

Figure 4.4: Conceptual integration of process safety and process security within the resilience engineering paradigm. The four resilience capabilities form a continuous cycle through which indicators bridge risk and disruption management across both domains.

Figure 4.4 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 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.

4.3 Methodology

4.3.1 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 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.

i. **Foundational synthesis from authors' prior work**: (Ab Rahim, Reniers, Yang, 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 4.2, 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.

These four stages formed a sequential yet iterative process through which the RoPSS framework and its indicator system were progressively developed and refined.

4.3.2 Expert interviews with scenario-based elicitation

Data were collected through semi-structured interviews with 16 purposively selected experts to represent diverse professional backgrounds (**Table 4.1**): 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 (Eva Magnusson & Jeane 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.

Table 4.1. 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

Within these interviews, a scenario-based expert elicitation (Schoemaker, 1993) was adapted and 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 minutes. Although all six thematic areas were explored, the present chapter 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 for indicator refinement is summarized in **Figure 4.5**.

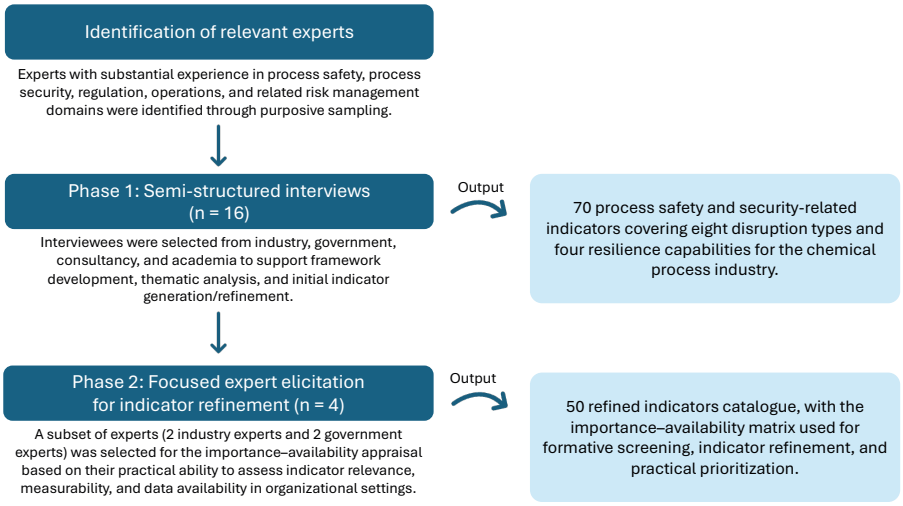

Figure 4.5: Expert selection process for semi-structured interviews and focused expert elicitation for indicator development and refinement

4.3.3 Data analysis and coding

Interview transcripts and field notes were analyzed using thematic analysis (Braun & 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.

4.3.4 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 Figure 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.

4.3.5 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 also provided follow-up comments and checks 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. The dataset can be accessed through this link: https://data.4tu.nl/datasets/cf35f909-c03b-4c9d-bdcd-2254f2bc6d06.

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.

4.4 Results

4.4.1 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 & Bieder, 2020a). 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.

i. 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.

ii. 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.

4.4.2 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.

4.4.2.1 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.

4.4.2.2 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.

4.4.2.3 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.

4.4.2.4 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.

4.4.3 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.

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.

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.

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.

By establishing shared objectives, organizations align safety and security values and enable coordinated decision-making under conditions that may involve conflicting imperatives.

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.

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.

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.

Figure 4.6 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.

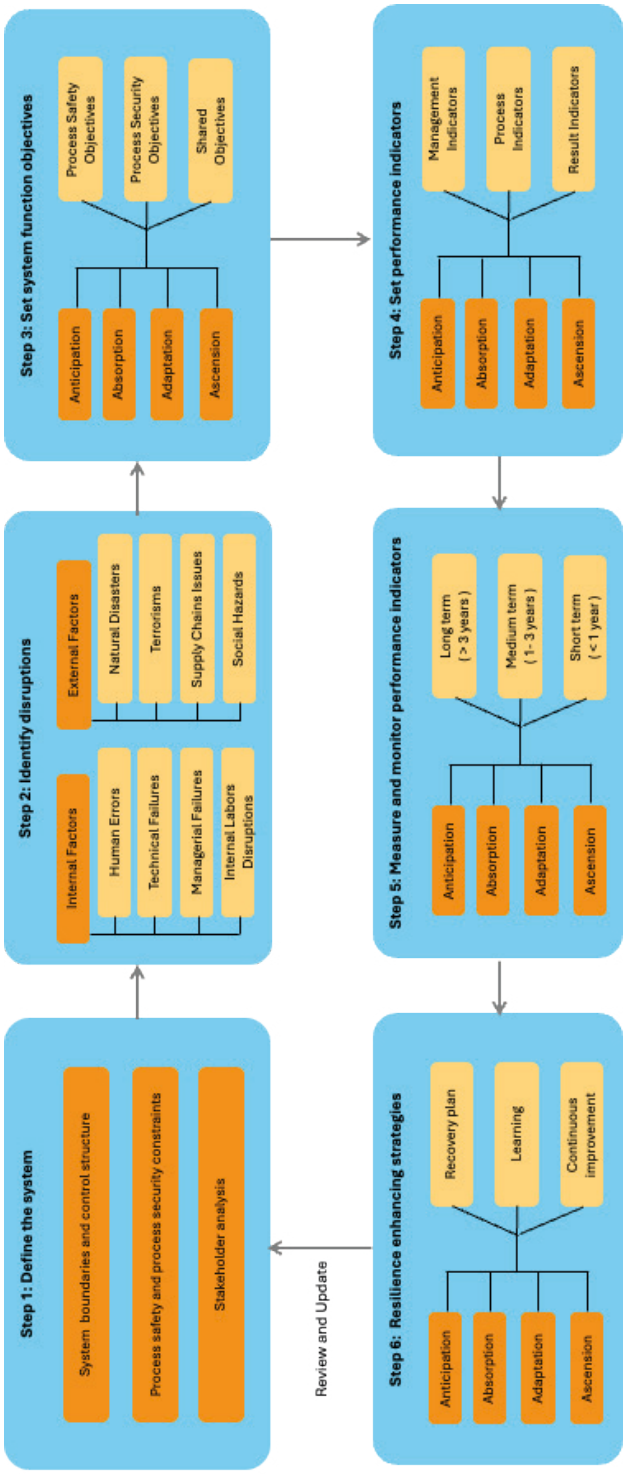

Figure 4.6: The six-step RoPSS framework integrates process safety, process security, and the 4As resilience capabilities.

4.4.4 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 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 3 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 in **Appendix C**.

Table 4.3. 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 investigation per year	Safety & Security
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

The examples in **Table 4.3** 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. Together, these three categories ensure that resilience is assessed not only through system reliability but also through organizational governance and learning maturity.

4.4.5 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 **Figure 4.7**. 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.

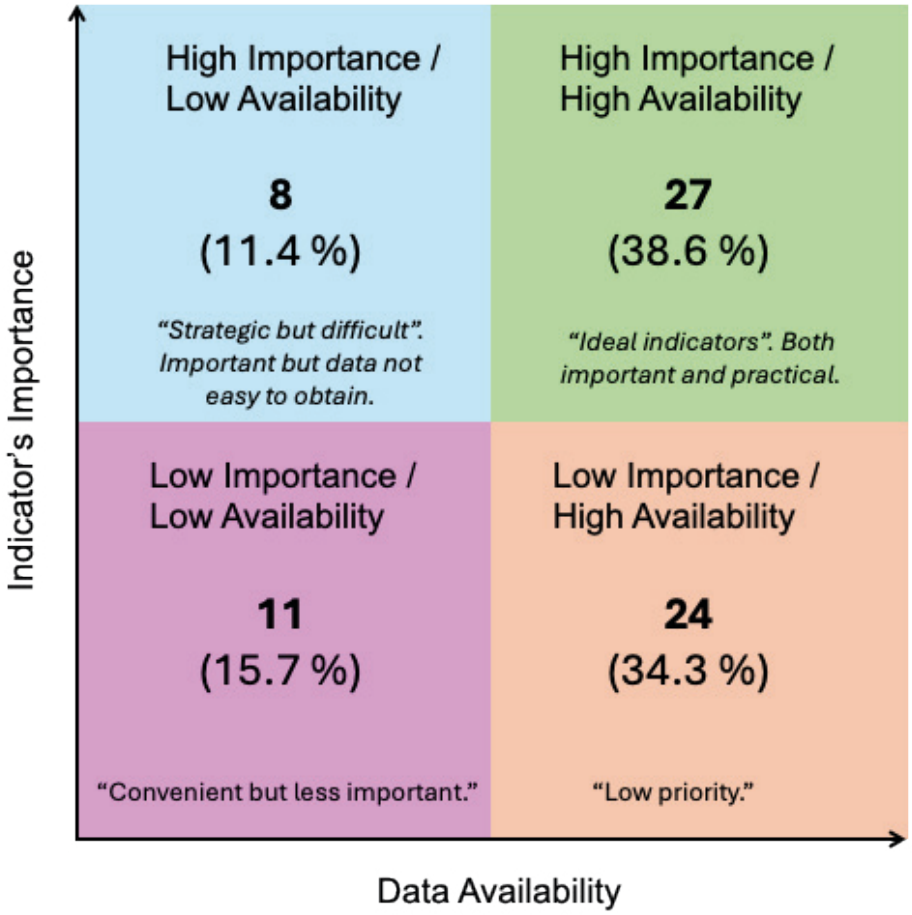

Figure 4.7. Importance–Availability Matrix for indicator assessment and practical prioritization (n = 70)

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 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 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.

Table 4.4: 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 to 10 indicators per disruption types across all four resilience capabilities.	Leaner and a more usable set for field implementation.

The refinement decisions informed by this analysis are summarized in **Table 4.4**. 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.

4.4.6 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. 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, 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, misconfigured firewall rules affecting SCADA connectivity, 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 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. Management indicators may include operator competence in recognizing cyber-physical anomalies or the adequacy of maintenance planning for hydrogen-handling equipment. Process indicators may monitor SCADA network reliability, emergency shutdown responsiveness, or the performance of hydrogen interlocks under fluctuating conditions. Result indicators could track the recurrence of similar compressor disturbances or the timeliness and completeness of corrective actions implemented after the event. Together, these indicators provide a balanced view of operational performance and organizational learning.

During **Step 5**, these indicators are measured and monitored to detect early warning patterns. 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, however, these patterns point to a shared underlying issue affecting both energy-isolation integrity and digital communication pathways. Identifying such trends would allow the plant

to take proactive measures rather than relying solely on incident-driven responses.

Finally, **Step 6** converts performance insights into resilience-enhancing strategies. Following a joint after-action review, the team plant may upgrades the outdated SCADA firmware, revise maintenance routines for compressor components, and initiate combined emergency drills involving operators, the safety team, and security personnel. Lessons from the event are incorporated into updated risk assessment procedures and 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, 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.

Taken together, the findings presented in this section show how the RoPSS framework brings together resilience capabilities, disruption classification, and performance measurement into a coherent management cycle. The expert insights, indicator architecture and catalogue, importance–availability assessment, and illustrative example collectively show that the framework is conceptually grounded and structured for future operationalization within the CPI.

4.5 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.

4.5.1 Conceptual and practical contributions

4.5.1.1 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.

4.5.1.2 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.

4.5.1.3 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.

4.5.1.4 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.

4.5.1.5 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 4.5** provides an illustrative alignment of the six RoPSS steps with familiar process safety and disaster management logic.

Table 4.5 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.

Table 4.5: 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

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.

4.5.2 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 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 chapter. 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.

4.6. Conclusion and recommendations

This chapter 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 key ways. 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. Case studies across different chemical facilities will be important for examining usability, assessing indicator feasibility, and refining the framework under real operational conditions. 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) or Bowtie, may also help clarify the distinct role of RoPSS as a resilience-oriented integrative management framework. 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.



4

Chapter 5



Operationalizing the RoPSS Framework: Application and Baseline Resilience Profiling in Chemical Plant Settings

Chapter 4 developed the Resilience-oriented Process Safety and Process Security (RoPSS) framework as an expert-informed conceptual framework designed for operationalization. It translated resilience engineering into a six-step management cycle supported by four resilience capabilities, eight disruption types, and a structured performance indicator catalogue. Chapter 5 moves from framework development to field application. It examines how RoPSS can be operationalized in two chemical plant settings and how the framework can generate baseline resilience profiles, evidence rationales, and resilience-enhancing strategies under real-world constraints of access, data availability, and governance boundaries.

This chapter is written with modifications based on the following research article: Ab Rahim, M. S., Reniers, G., Yang, M., Schmitz, P., & Mhd Yusop, M. Y. (2026). Operationalizing the RoPSS framework in chemical plants: Diagnostic profiles and methodological lessons from two case studies. Safety Science (Under Review)

ABSTRACT

Operationalizing integrated process safety–security management is challenging because organizations often lack practical tools that can be applied consistently across disruption types under real-world constraints on access, data, and governance. This chapter demonstrates how the Resilience-oriented Process Safety and Process Security (RoPSS) framework can be operationalized in chemical plants to generate baseline resilience profiles for integrated process safety–security sense-making. Using a multiple-case study design, RoPSS was applied to two cases in the chemical process industry under contrasting implementation conditions. Plant M used a cross-functional, workshop-based application in a single-operator plant, while Plant N used an iterative, key-informant-led application under bounded access in a multi-operator industrial complex. The same disruption-organized questionnaire package and indicator catalogue were used in both cases, structured across eight disruption types and four resilience capabilities: Anticipation, Absorption, Adaptation, and Ascension. Indicators were scored on an anchored five-point scale with brief evidence rationales; non-assessable items were marked as N/A and excluded from aggregation. Operationalization yielded comparable baseline outputs in each case, including auditable scoring trails, capability radar profiles, disruption-by-capability heatmaps, and qualitative resilience-enhancing strategies. The study highlights practical implementation insights, including selective qualitative scoring, two-step assessment for maturity-dependent indicators, and the need to document ownership boundaries and evidence expectations to support interpretable profiling.

5. OPERATIONALIZING THE ROPSS FRAMEWORK

5.1 Introduction

5.1.1 From conceptual integration to operational use

Chemical process industries (CPI) operate as complex socio-technical systems (Yang et al., 2023), in which hazardous materials, tightly coupled equipment, and human–organizational interactions can lead to severe consequences when failures occur. Traditionally, organizations manage these risks through process safety systems focused on preventing and mitigating unintentional events (e.g., equipment failure, human error) and through process security arrangements aimed at protecting facilities against intentional threats (e.g., sabotage, terrorism, cyberattacks) (Ab Rahim et al., 2025; El-Kady et al., 2023). However, these two domains often evolve under different professional traditions, regulatory regimes, and operational logics, which encourage parallel risk assessments and fragmented organizational routines rather than integrated decision-making (Ylönen et al., 2022).

This fragmentation is increasingly challenging because safety and security risks can interact through shared infrastructures and dependencies, including control systems, operational technology, human resources, contractor interfaces, and managerial processes (Hansen & Antonsen, 2024; Kenneth & Gould, 2020). A disturbance originating in one domain may therefore influence vulnerabilities and response capacity in the other, and organizational attention can be pulled toward compliance- or incident-driven priorities instead of developing a coherent, cross-domain capability over the full disruption cycle (Pettersen Gould & Bieder, 2020b; Schulman, 2020). This operational emphasis is consistent with resilience engineering, which frames resilient performance in terms of core system abilities (e.g., anticipating, monitoring, responding, and learning) and has motivated practical assessment approaches that translate these abilities into measurable organizational routines (Hollnagel, 2006; Woods, 2015).

Prior work in this thesis has progressed from identifying the conceptual gap to developing an operational framework. Chapter 2 showed that while process safety risk assessment methods are comparatively mature, process

security and resilience assessment in the CPI remain less developed, and joint safety–security assessment using a resilience-oriented approach remains limited. Chapter 3 then reported practitioner perspectives on integration, identifying perceived benefits such as reduced redundancy, optimized resource use, and improved risk management, alongside persistent barriers such as siloed communication, knowledge gaps, and resource constraints. Building on these findings, Chapter 4 developed the Resilience-oriented Process Safety and Process Security (RoPSS) framework, translating resilience into a six-step management cycle supported by a structured indicator catalogue and introducing Ascension as an evolutionary capability that explicitly incorporates recovery, learning, continuous improvement, and prevention.

Against this backdrop, this chapter focuses on the operationalization of RoPSS in real chemical plant settings. The practical value of resilience-oriented frameworks depends on their ability to be translated into feasible assessment procedures, evidence requirements, scoring practices, diagnostic outputs, and improvement actions within organizational contexts. Recent resilience research similarly emphasizes the need to translate resilience concepts into context-tailored assessment tools that can support practical organizational use (Afonso-Fernandes et al., 2026). This chapter examines this operationalization challenge through two chemical plant case studies, reporting the baseline resilience profiles and implementation insights that emerged from applying RoPSS as a structured diagnostic and sense-making tool under real-world constraints of access, data availability, and governance boundaries. In doing so, the chapter contributes to the methodological understanding of how integrated and resilience-oriented process safety–security frameworks can be translated into auditable, boundary-aware, semi-quantitative assessment practice.

5.1.2 Research objective and guiding questions

Building on the framework-development work presented in Chapter 4, this chapter shifts attention from conceptual design to practical use. The focus is on how RoPSS can be applied in real chemical plant settings, what kinds of baseline resilience profiles it can generate, and what implementation insights emerge when the framework is used under realistic constraints of access, data availability, and governance boundaries. In this chapter, sense-making refers to the process through which complex, ambiguous, or

fragmented circumstances are turned into an explicitly articulated situation that can provide a basis for action (Weick & Sutcliffe, 2005). Accordingly, the chapter is guided by the following objective and research questions.

Objective

This study examines how the RoPSS framework can be operationalized in chemical plant settings to support integrated process safety–security sense-making and diagnostic use.

Research Question (RQ)

How can the RoPSS framework be operationalized in chemical plant settings to support integrated process safety–security risk management?

Sub-Research Questions (SRQ)

SRQ1. What baseline resilience profiles emerge when applying the RoPSS framework in two chemical plant contexts?

SRQ2. What implementation insights emerge regarding the use of RoPSS as a diagnostic and sense-making tool under real-world access, evidence, and governance constraints?

5.1.3 Scope and boundaries of the study

This chapter is positioned as an operationalization and use case study. It documents the implementation process, the pragmatic adaptations made during application, and the profiling outputs produced, including baseline resilience profiles and structured reflections. This positioning is consistent with calls for case-based evidence on how resilience-oriented assessment approaches can be embedded in real organizational settings (Klockner & Meredith, 2020; Patriarca, Di Gravio, et al., 2018).

Several boundaries are therefore explicit. First, the chapter does not evaluate indicator adequacy, predictive validity, or effectiveness outcomes. Instead, it treats RoPSS as a structured lens for applying integrated process safety–security thinking in practice and for generating baseline profiles to support organizational reflection. Second, the analysis is conducted at the plant/system level, focusing on how organizational arrangements, routines, and capabilities support or constrain integrated management, rather than estimating scenario probabilities or quantifying risk in a probabilistic sense. Third, the work is case-based. The two plants are used to provide

contrasting implementation contexts and to illustrate the transferability of the operational process across settings, not to perform a country-level comparison or benchmark plant performance.

In addition, the chapter treats assessment boundaries as a core operationalization issue. Where relevant practices or data were governed outside plant-level ownership, such as site-level or industrial-park security functions, this was documented and interpreted as an operationalization constraint rather than a plant performance deficit. Similarly, non-assessable items were marked as N/A and excluded from aggregation, while retained as meaningful information about evidence availability, applicability, and ownership boundaries. The resulting scores and profiles are therefore interpreted as diagnostic baseline representations, not as precise interval-level measurements or definitive performance rankings.

Within these boundaries, this chapter presents three main outputs from the operationalization process: (i) a transparent account of how RoPSS was applied in two industrial settings, (ii) baseline resilience profiles generated as diagnostic outputs, and (iii) implementation insights on the use of RoPSS as a sense-making tool during field application. These outputs are interpreted as context-dependent evidence of operational use, rather than as validation or benchmarking.

5.2. Framework overview and implementation context

5.2.1 Overview of the RoPSS framework

As developed in Chapter 4, the Resilience-oriented Process Safety and Process Security (RoPSS) framework (**Figure 5.1**) supports integrated management of process safety and process security in CPI by applying a resilience engineering perspective (Ab Rahim et al., 2026). Rather than treating safety and security as separate domains managed through parallel routines, RoPSS provides a common structure for examining how organizational arrangements, technical safeguards, and operational practices jointly enable a plant to anticipate, withstand, adapt to, and improve following a broad range of disruptions.

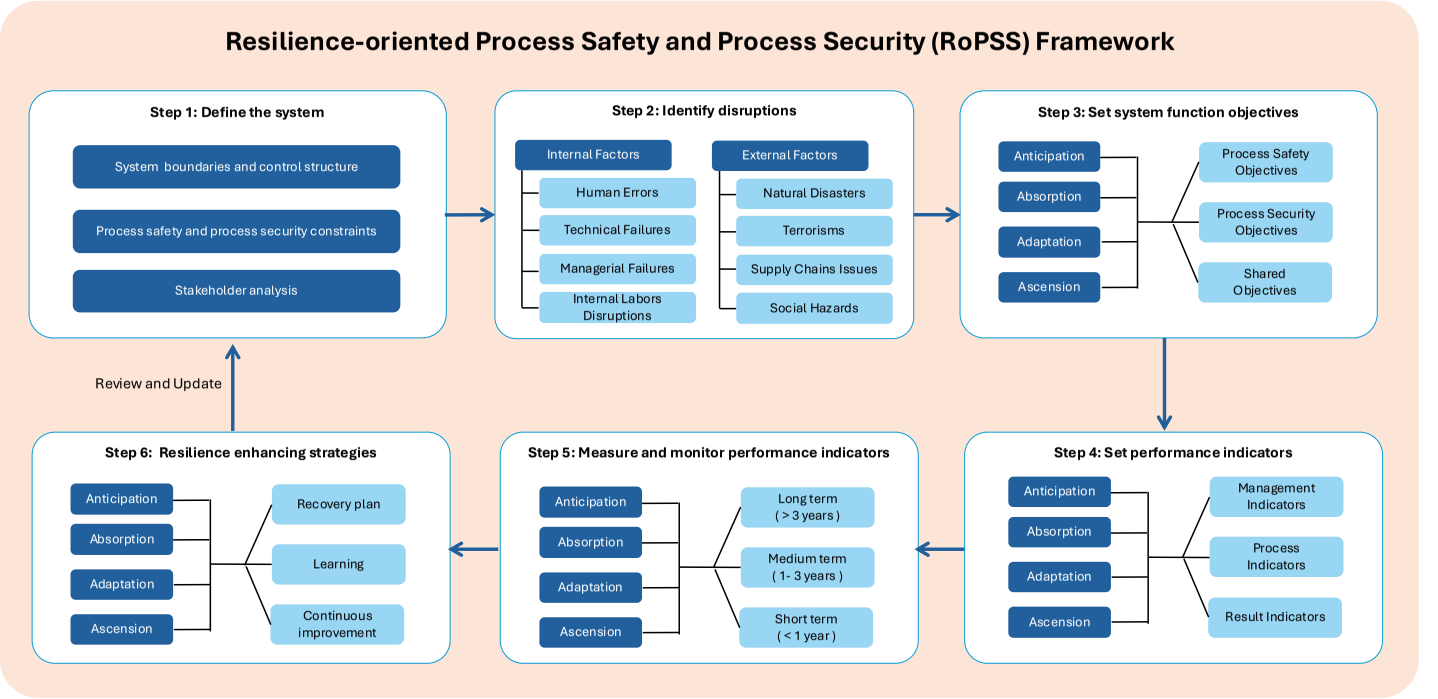

Figure 5.1. The six-step RoPSS framework, which integrates process safety, process security, and the four resilience capabilities.

RoPSS conceptualizes resilience through four capabilities, referred to as the 4As: Anticipation, Absorption, Adaptation, and Ascension. Anticipation concerns proactive identification of hazards and threats and preparation for their occurrence. Absorption refers to maintaining critical functions and containing consequences during disruptions. Adaptation captures the ability to adjust operations and reconfigure resources in response to changing conditions. Ascension extends beyond recovery by emphasizing learning, institutional reinforcement, and sustained strengthening of safety and security performance over time (Ab Rahim et al., 2026; Mentges et al., 2023).

To translate these capabilities into operational practice, RoPSS is structured as a six-step continuous management cycle. First, the organization defines system boundaries and critical functions, clarifying what "normal performance" means within the plant context. Second, potential disruptions are identified and organized to ensure coverage of both accidental and intentional sources of disturbance. Third, system function objectives are articulated for each resilience capability, specifying what the organization seeks to achieve across the 4As. Fourth, performance indicators are selected to support semi-quantitative assessment of how well these objectives are enabled in practice. Fifth, indicators are assessed and monitored using a structured scoring approach accompanied by brief qualitative rationales, generating a baseline resilience profile that can be revisited over time. Sixth, resilience-enhancing strategies are proposed to address identified gaps and priorities, and the cycle is periodically reviewed as part of continuous organizational learning (Ab Rahim et al., 2026).

A key feature of RoPSS is its broad view of disruption sources. In this study, the application considered eight disruption categories: human errors, technical failures, managerial failures, internal labour disruptions, natural disasters, terrorism/sabotage, supply chain disruptions, and external social hazards. This structuring ensures that process safety and process security concerns are examined within a single assessment logic, while still allowing emphasis to be tailored to local context and risk landscape.

Operationally, RoPSS is implemented through an indicator catalogue organized by disruption type, resilience capability, and indicator type (management, process, and result indicators). This structure supports deliberative assessment in which practitioners assign ratings based

on available evidence and professional judgement, alongside narrative explanations that capture reasoning and contextual qualifiers. The resulting outputs are not intended as predictive risk estimates; rather, they provide a diagnostic baseline that supports cross-functional sense-making, reveals potential safety–security interdependencies, and informs prioritisation of improvement actions.

5.2.2 Case study selection and context

This study adopts a multiple case study design to demonstrate how the RoPSS framework can be operationalized in real plant settings under contrasting implementation conditions. Two chemical plants were selected to provide variation in (i) organizational setting and governance arrangements, (ii) access conditions and modes of engagement, and (iii) the practical pathways through which integrated process safety–security sense-making can be facilitated. The intention is not to conduct a national comparison, but to examine how RoPSS can be applied across different organizational contexts and constraints.

Plant M: Embedded operationalization in a single-operator plant.

Plant M is a chlor-alkali manufacturing facility located in Malaysia. It operates in a major-hazard context involving hazardous chemical production and associated storage and transfer activities. RoPSS implementation was conducted in two phases. Phase 1 (30 July–2 August 2024) focused on on-site engagement to establish scope, boundaries, and evidence sources. Evidence familiarization was supported through (i) walkdowns and control-room/field observations, and (ii) demonstrations of operational control systems, including permit-to-work (PTW) routines and audits and non-routine work controls such as Job Safety Analysis (JSA) and isolation/lockout certification. Cross-functional discussions and interviews were conducted in parallel to clarify how these controls were applied in practice. Phase 2 (6–7 May 2025) consisted of a structured two-day facilitated workshop that applied RoPSS through disruption-specific discussions aligned to the eight disruption categories, enabling systematic engagement with the indicator set and consolidation of operationalization outputs. Across both phases, the application considered the overall plant system and two focal areas selected to ground the assessment in concrete contexts: the HCl synthesis unit and the methyl chloride storage tank area.

Plant N: Bounded-access operationalization in a multi-operator industrial complex.

Plant N is a caprolactam manufacturing site located within a large integrated industrial complex in the Netherlands. It is characterized by a multi-operator cluster setting. In this environment, installations are linked through technical and organizational interdependencies and shared infrastructure, and certain functions (e.g., site-wide emergency planning interfaces and elements of access control) are coordinated at the complex level, while individual site users remain responsible for the safe operation and compliance of their own installations. In contrast to Plant M, RoPSS operationalization in Plant N occurred under more bounded access conditions. Engagement was facilitated primarily through a single key informant (the site HSE Manager) and conducted through iterative online meetings and in-person discussions in a meeting-room setting at the industrial complex, supplemented by contextual familiarization through an external site visit. Plant N is therefore treated as a bounded-access implementation case, illustrating how RoPSS can be applied when direct cross-functional participation is limited by confidentiality, access, and multi-operator governance constraints.

Both plants operate under major-hazard governance regimes that require structured arrangements for preventing and managing low-probability, high-consequence events, which shaped the availability of documents and organizational routines used during RoPSS application. In Plant M, major hazard management is governed under Malaysia's Occupational Safety and Health Act 1994 and the Control of Industrial Major Accident Hazards (CIMAH) Regulations 1996 (DOSH, 1996). In Plant N, major-hazard obligations fall under the Netherlands' implementation of the EU Seveso III regime (European Union, 2012) and related Dutch legislation, with general occupational safety framed by the Working Conditions Act (Nederlandse Arbeidinspectie, 2026). In both settings, process security is also relevant in practice through arrangements such as access control, site rules, and information security controls, which formed part of the operational context for applying RoPSS. Particularly in European settings, cybersecurity governance is increasingly formalized through NIS2, which strengthens organizational duties for cybersecurity risk management and incident reporting in critical sectors (European Union, 2022).

Taken together, the two cases provide complementary implementation conditions. Plant M illustrates an embedded, cross-functional operationalization pathway supported by on-site observation and facilitated workshop deliberation, whereas Plant N illustrates a key-informant-led pathway shaped by confidentiality constraints, organizational gateways, and multi-operator governance. This contrast enables a practice-oriented examination of how RoPSS can be operationalized under realistic conditions encountered in CPI, while maintaining caution against interpreting the results as direct performance benchmarks between the two plants.

5.2.3 Scope of framework application

The RoPSS framework was applied in both case studies as a structured, semi-quantitative diagnostic approach to support integrated process safety–security sense-making. The purpose was to examine how the same instrument could be operationalized under contrasting plant contexts and access conditions. To maintain a clear operationalization focus, the application emphasized: (i) defining system boundaries and critical functions, (ii) considering a broad set of disruption sources, (iii) applying a structured indicator set through deliberative scoring supported by available evidence, and (iv) producing baseline resilience profiles intended for organizational reflection and prioritization.

In both plants, the primary unit of analysis was the plant-level process safety–security management system (i.e., governance arrangements, routines, and cross-functional interfaces) as these relate to the four resilience capabilities. To ground operationalization in concrete operational contexts and to support evidence-informed discussion, each case study also included focal areas reflecting salient risk interfaces and practical evidence availability.

In Plant M, RoPSS was applied at two complementary levels: (i) the overall plant system relevant to integrated process safety–security management and (ii) two focal areas selected to anchor discussions and evidence gathering, namely the HCl synthesis unit and the methyl chloride storage tank area. The HCl synthesis unit provided a bounded process context where routine operational control, maintenance integrity, and emergency preparedness practices could be examined. The methyl chloride storage area provided a high-hazard storage/transfer context that foregrounded containment, detection, access control, and operational discipline.

In Plant N, application was scoped at three complementary levels that reflect the industrial-complex setting and the access conditions of the study: (i) site-level arrangements relevant to integrated safety–security management within a multi-operator industrial complex (including interfaces with site-wide emergency planning and access control), (ii) the core manufacturing process representing the plant's main production system, and (iii) the logistics and loading interface, where material movements, contractor presence, and external interactions shape both process safety exposure and security vulnerability. This scoping supported practical sense-making across organisational layers and reflected the fact that deep equipment-level auditing was not the intention of this operationalization study.

In both cases, the application considered eight disruption categories consistent with RoPSS (Ab Rahim et al., 2026). It consists of human errors, technical failures, managerial failures, internal labour disruptions, natural disasters, terrorism and sabotage, supply chain disruptions, and external social hazards. These categories were used as prompts to ensure that both accidental and intentional sources of disturbance were addressed within a common structure and to support cross-functional discussion beyond traditional safety-only lenses. The assessment was conducted as a baseline snapshot based on evidence available during the case study engagements and participants' professional judgement. Discussion covered routine operations and disruption conditions across preparedness (anticipation), immediate response and containment (absorption), operational adjustment (adaptation), and learning and improvement (ascension). The resulting profiles are therefore interpreted as context-dependent baseline representations intended to guide organizational reflection rather than as benchmark scores.

Several aspects were excluded to align with the operationalization scope. First, RoPSS was not used to estimate event probabilities, quantify individual risk, or produce quantitative societal risk contours. Second, no attempt was made to validate indicator completeness, define indicator weighting schemes, or demonstrate predictive accuracy. Third, the study did not aim to compare national regulatory performance or to generalize findings beyond illustrating practical framework use under contrasting implementation conditions. These exclusions are consistent with RoPSS

being applied here as a diagnostic and sense-making tool; formal validation and refinement are addressed as directions for work.

5.3. Methodology

5.3.1 Research design

A multiple case study design (Yin, 2017) was used to demonstrate how the RoPSS framework can be operationalized and applied in chemical process industry settings, and to document the resulting baseline profiles and implementation insights. Two cases were selected to represent contrasting implementation conditions, particularly in terms of organizational setting and research access. The purpose of this design is to demonstrate operational use rather than the validation of indicator adequacy, completeness, or effectiveness.

RoPSS was operationalized using the same instrument package in both cases, but through different engagement pathways aligned with the access conditions of each plant. In Plant M, operationalization combined an initial on-site engagement to establish scope and evidence sources with a facilitated cross-functional workshop to complete scoring across disruption categories. In Plant N, operationalization relied on iterative structured engagement with a knowledgeable key informant, supported by available documents, structured questionnaires, and in-person discussions.

These two pathways are intentionally treated as contrasting operationalization modes rather than methodologically equivalent routes for direct performance comparison. Plant M illustrates a broader cross-functional application pathway, while Plant N illustrates a bounded-access pathway shaped by confidentiality constraints, organizational gateways, and multi-operator governance realities. Accordingly, cross-case interpretation is used to compare implementation patterns, diagnostic outputs, and evidence-boundary issues. **Table 5.1** summarizes the implementation mode, scope, data sources, and scoring approach for Plant M and Plant N.

Table 5.1: Summary of case study implementation and data collection approach

Method element	Plant M	Plant N
Implementation mode	Embedded, cross-functional operationalization	Key-informant-led operationalization under bounded access
Primary access pathway	Direct access and cooperation (multi-function participation)	Single key contact (site HSE Manager), with supervisor involved in selected sessions
Fieldwork timeline	Phase 1: 30 Jul–2 Aug 2024 (on-site engagement). Phase 2: 6–7 May 2025 (facilitated workshop)	Iterative engagement Sep 2024–Jun 2025. Key synchronous engagements: 6 Sep 2024; 10 Dec 2024; 14 Mar 2025; 27 Mar 2025. Structured questionnaires completed May–Jun 2025
Unit and scope of application	Overall plant system, HCl synthesis unit, and methyl chloride storage area	Site-level arrangements, core manufacturing process, and logistics/loading interfaces (bounded by access conditions)
Common instruments across cases	Same RoPSS indicator set and structured questionnaires, completed in a facilitated workshop (6–7 May 2025)	Same RoPSS indicator set and structured questionnaires, completed through a questionnaire package supported by iterative, documented discussions (May–Jun 2025)
Data sources	Document review, interviews, observations/ walkdowns, and facilitated workshop outputs	Document review, structured discussions, external site familiarisation and meeting-room sessions, and disruption-specific questionnaires
Facilitated application	Structured, disruption-led workshop aligned to eight disruption categories	Structured deliberation with key informant, supported by in-person case engagement including process briefing and site familiarisation
Scoring approach	Deliberative consensus in a cross-functional group, supported by documented evidence and brief rationales	Deliberative consensus with a key informant, supported by documented evidence, brief rationales, and follow-up exchanges
Scoring scale	1–5 scale with indicator-specific anchors	1–5 scale with indicator-specific anchors

Missing data handling	"N/A" used where not assessable or not applicable; excluded from averages	"N/A" used where not assessable or not applicable; excluded from averages
Aggregation and outputs	Capability averages (A1–A4), disruption × capability heatmaps, indicator-type summaries (M/P/R), qualitative rationales, and Step 6 strategy suggestions	Capability averages (A1–A4), disruption × capability heatmaps, indicator-type summaries (M/P/R), qualitative rationales, and Step 6 strategy suggestions
Triangulation strategy	Cross-functional perspectives combined with documents, on-site observations, and workshop deliberation	Iteration over time combined with documentary triangulation, multiple synchronous sessions, and questionnaires covering all disruption types
Known constraints and mitigation	Potential workshop dynamics (e.g., dominant voices), mitigated through facilitation, anchor-based scoring, and recorded rationales	Reliance on a key informant, mitigated through repeated engagement, an auditable scoring trail, document support, and structured questionnaires

5.3.2 Data sources

Four data sources supported RoPSS application across the two cases.

i. **Document review.** Documents were used to characterize organizational arrangements and to support evidence-informed scoring. These included major hazard and safety management artifacts, relevant management system documentation, and (where accessible) industrial-complex materials that contextualized governance arrangements.
ii. **Interviews and structured discussions.** Semi-structured interviews and structured discussions were used to elicit how safety and security are organized, how disruptions are anticipated and managed, and what evidence exists for assessing indicators. Engagement covered multiple functions where access was permitted and relied on a key informant under bounded access conditions.
iii. **Observations and site familiarization.** Walkdowns and observations (where available) complemented documentary and interview evidence by providing contextual understanding of operational routines and non-routine work controls. Where direct observation was constrained, contextual familiarization was supported through in-person engagement and structured briefings.
iv. **Facilitated RoPSS application sessions and outputs.** RoPSS application produced completed scoring sheets, brief qualitative rationales supporting each score, and open-ended inputs such as candidate resilience-enhancing strategies and usability reflections.

5.3.3 RoPSS operationalization procedure

RoPSS was applied using a structured procedure aligned with its six-step management cycle.

Step 1 – System boundaries and focal areas were agreed for each case, as described in Section 5.2.3.

Step 2 – Eight disruption categories were used as prompts to ensure coverage of both accidental and intentional disturbances.

Step 3 – Process safety and process security objectives were discussed using the four resilience capabilities (Anticipation, Absorption, Adaptation, Ascension) as an organizing lens.

Step 4 – The indicator architecture and catalogue developed in Chapter 4 were used as the basis for assessment; indicators were interpreted within the case scope and access conditions.

Step 5 – Indicators were scored using a deliberative semi-quantitative approach.

Step 6 – Participants proposed actions/ projects/ programs linked to scored gaps and contextual priorities. These were recorded as qualitative outputs to support diagnostic reflection and improvement planning.

The procedure was applied flexibly enough to accommodate different access conditions while preserving a common structure across the two cases. This allowed both applications to generate comparable types of outputs, including scored indicators, brief evidence rationales, baseline profiles, and candidate resilience-enhancing strategies.

5.3.4 Indicator scoring protocol, missing data handling, and aggregation

Indicators were assessed on a five-point (1–5) scale using indicator-specific anchors provided in the RoPSS catalogue. Indicator-specific anchors were used because indicators vary in nature, including the existence of arrangements, maturity of implementation, frequency of activities,

and outcomes. A single universal anchor set was therefore considered inappropriate.

Scoring followed a deliberative process. To reduce arbitrariness, scoring proceeded as follows: (i) the indicator definition and anchor descriptions were reviewed, (ii) relevant evidence was discussed (documents, records, observations where available, and professional judgement), and (iii) a single score was recorded alongside a brief written rationale. Where initial views differed, discussion returned to the anchor definitions and evidence expectations for each level. If uncertainty remained due to limited evidence, scores were assigned conservatively, toward the lower plausible level, and the uncertainty was noted in the rationale.

The 1–5 scores are treated as anchored ordinal ratings rather than precise interval-level measurements. Mean values were used as transparent descriptive summaries to support visualization and pattern recognition, while medians, N/A coverage, and written rationales were retained to support interpretation. The resulting profiles are therefore interpreted diagnostically, with emphasis on relative patterns, evidence explanations, and follow-up priorities.

When an indicator could not be assessed due to insufficient evidence or because it was not applicable to the defined system boundary, it was marked as “N/A.” N/A items were excluded from aggregation, such that averages were calculated only over indicators with valid scores. At the same time, N/A markings were retained as part of the operationalization output because they provide information about evidence availability, applicability, and ownership boundaries.

Scores were aggregated into baseline profiles in three complementary ways. First, indicator scores were summarized into average values for the four resilience capabilities to produce a capability profile for each plant. Second, scores were organized into disruption × capability matrices and visualized as heatmaps to identify disruption-specific strengths and fragile areas within each capability. Third, indicator-type patterns were examined using the built-in Type labels (Management, Process, Result) to compare how governance-oriented, practice-oriented, and outcome-oriented indicators contributed to the baseline profile. In parallel, qualitative rationales and open-ended responses were synthesized descriptively

to capture recurring implementation issues, such as indicator clarity and evidence availability, and to collate proposed resilience-enhancing strategies as Step 6 outputs.

Aggregation used transparent, unweighted averages to maintain interpretability and to keep the focus on baseline profiling and operational use. The development of weighting schemes is recognized as a relevant methodological extension, but is treated as future work beyond the present study.

5.3.5 Context mapping variables

To support the interpretation of the implementation processes and baseline profiles, a brief context map was compiled for each case. The mapping consisted of structured notes (and where available, supporting documents) organized under five headings: (i) organizational setting and governance (e.g., single-operator site versus multi-operator industrial complex, allocation of responsibilities between site users and complex-level functions), (ii) safety and security roles and coordination mechanisms (e.g., ownership of access control, security risk analysis, emergency interfaces, and follow-up loops), (iii) major-hazard governance context and evidence infrastructure (e.g., Seveso-type obligations and the presence of formal safety management and emergency preparedness artifacts), (iv) operational scope and complexity factors that shape evidence availability and implementation feasibility (e.g., contractor interfaces, logistics/loading activities, and site interdependencies), and (v) access pathway and implementation feasibility conditions.

The context map was used in three ways. First, it supported boundary setting by clarifying what could be assessed at plant level versus what was governed externally, which helped make “N/A” decisions consistent. Second, it supported interpretation of baseline patterns by explaining why certain disruption–capability cells appeared strong or weak within the assessed boundary, for example where ownership of long-cycle security activities sat outside the plant or where interfaces such as logistics and contractors increased operational complexity. Third, it supported interpretation of implementation enablers and constraints by linking differences in operationalization mode (cross-functional workshop versus bounded key-informant pathway) to the governance and access conditions of each case. Overall, the mapped variables were used to strengthen

feasibility and interpretability of the results rather than to evaluate regulatory performance. A summary of the context map headings and example observations is provided in **Appendix D.**

5.3.6 Researcher role and confidentiality

The researcher acted as a facilitator of structured discussions and as a recorder of scores and rationales. The objective of facilitation was to support consistent interpretation of RoPSS concepts and indicators and to document practical considerations in applying the framework. This facilitation supported transparency and consistency during application, although it did not constitute a formal inter-rater reliability or independent calibration procedure.

Organizational confidentiality was maintained through anonymization of case organizations and non-disclosure of identifying operational details. To support auditability and transparency of the operationalization process, a detailed inventory of operationalization artifacts and outputs produced in each case study is provided in **Appendix E.**

5.4. Results

5.4.1 Operationalization of the RoPSS framework

RoPSS was operationalized in both case studies using the same disruption-organized questionnaire package, producing comparable scoring records despite contrasting access conditions (Ab Rahim et al., 2026). In each case, operationalization generated three tangible outputs: (i) completed indicator scores accompanied by brief written rationales and “N/A” markings where assessment was not possible, (ii) baseline resilience profiles (capability averages and disruption-by-capability visual profiles), and (iii) Step 6 resilience-enhancing strategies captured as qualitative proposals. The two cases differed primarily in the implementation pathway; cross-functional workshop-based operationalization in Plant M versus iterative key-informant–led operationalization under bounded access in Plant N. However, both yielded an auditable scoring trail suitable for diagnostic profiling.

Across both cases, several practical adaptations were important in enabling the use of the instrument in real organizational settings. First, some indicators were assessed using qualitative 1–5 judgements in instances

where routine data systems could not support reliable quantification or where "available numbers" risked misrepresenting the underlying practice. Second, a two-step assessment logic was used for selected indicators: the underlying quality or maturity of the practice was assessed before quantitative measurement was considered meaningful. Third, facilitation and iterative review were used to clarify indicator wording, anchor interpretation, and evidence expectations, thereby supporting internal consistency across disruption domains and informants.

Overall, these operationalization experiences indicate that RoPSS can be applied through both time-bounded, workshop-based formats and bounded-access, iterative formats, provided that the process maintains structured interpretation of anchors, explicit documentation of rationales (including reasons for "N/A"), and sufficient iterative engagement to resolve ambiguities. The need for selective qualitative scoring and occasional two-step assessment further highlights the value of measurement flexibility when applying integrated safety–security indicators within existing organizational data infrastructures.

5.4.2 Baseline resilience profiles

5.4.2.1 Resilience capability profiles

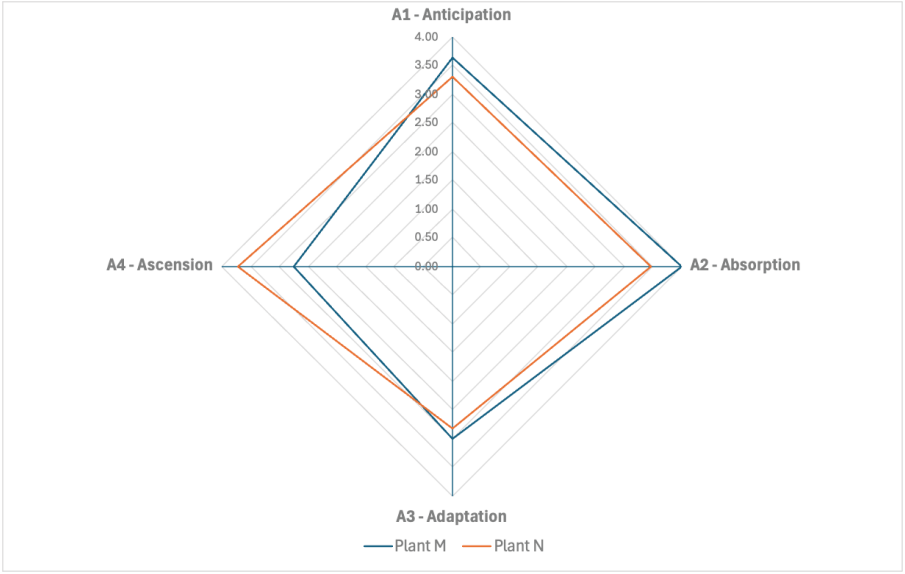

Figure 5.2: Capability profile radar chart (mean scores; NA excluded)

Figure 5.2 presents the capability-level baseline profiles (A1–A4) for Plant M and Plant N. Capability scores were computed by pooling all relevant performance indicators (PIs) ratings across the eight disruption types and reporting both mean and median values (excluding "N/A"), as descriptive summaries of the baseline profile.

Plant M exhibits its strongest capability in A2 (Absorption) (mean = 4.00; median = 4) and a solid score in A1 (Anticipation) (mean = 3.64; median = 4), whereas A3 (Adaptation) (mean = 3.00; median = 3) and A4 (Ascension) (mean = 2.75; median = 3) are comparatively lower. Plant N shows its strongest capability in A4 (Ascension) (mean = 3.73; median = 4), followed by A2 (Absorption) (mean = 3.46; median = 4) and A1 (Anticipation) (mean = 3.31; median = 4), while A3 (Adaptation) is comparatively weaker (mean = 2.83; median = 3).

Overall, the profiles indicate different resilience emphases under the same RoPSS assessment structure. Plant M's higher A2 and A1 scores suggest comparatively stronger short-term robustness and readiness across assessed disruption domains, whereas Plant N's higher A4 score indicates comparatively stronger longer-cycle embedding and institutionalization of improvements. The comparatively lower A3 score in Plant N points to a weaker adaptation loop within the assessed boundary, particularly for indicators reflecting systematic updating or upgrading following disruptions. Capability scores are therefore reported using both the mean and the median (excluding "N/A") as a transparent descriptive summary of the baseline profile, and the resulting patterns are interpreted as diagnostic signals to guide deeper disruption-level examination in the subsequent subsections rather than as precise measurements.

5.4.2.2 Disruption-by-capability heatmaps

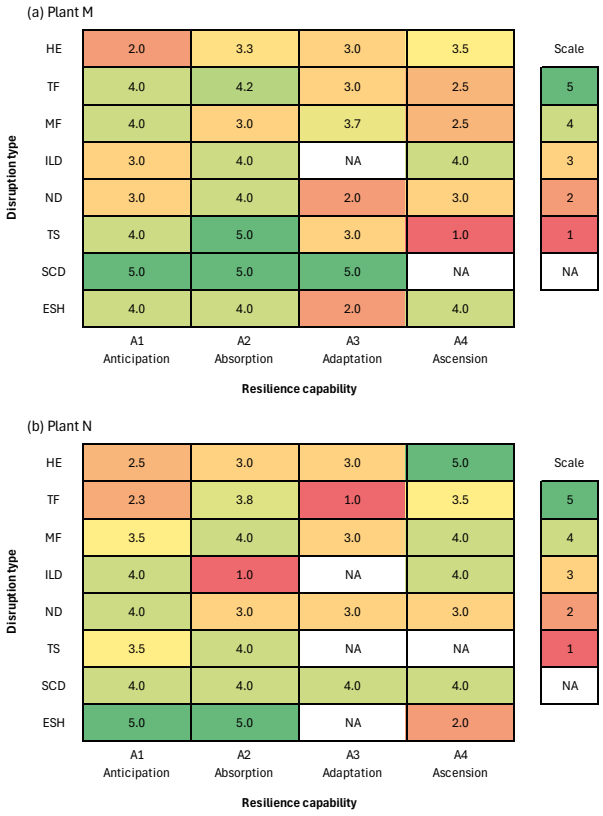

Figure 5.3. Disruption vs. capability heatmap (mean scores) for (a) Plant M and (b) Plant N.

Figure 5.3 presents disruption-by-capability heatmaps for Plant M and Plant N, with disruption types on rows and resilience capabilities (A1–A4) on columns. Each cell represents the mean of the PI ratings mapped to the corresponding disruption–capability combination (excluding "N/A"). This view complements the capability radar by indicating where strengths and weaknesses concentrate within specific disruption domains rather than only at the aggregated capability level.

For Plant M, the heatmap highlights consistently high performance in supply chain-related capabilities, with SCD–A1, SCD–A2, and SCD–A3 all scoring 5.0, indicating highly institutionalized practices in supplier assurance, buffering/continuity arrangements, and improvement actions within the assessed scope. From a business continuity management (BCM)

perspective (ISO, 2019), this pattern suggests that Plant M has embedded preventive and absorptive continuity practices around supply resilience as part of routine organizational functioning. Technical failure prevention and continuity measures are also comparatively high, particularly TF–A2 (mean = 4.2), consistent with robust protection layers and established routines that support operational continuity during equipment-related disruptions.

In contrast, Plant M exhibits a pronounced weakness for Terrorism/Sabotage under Ascension (TS–A4), scored at 1.0. Interpreted through a BCM lens, this indicates a more structural gap than a simple operational weakness: low-probability, high-impact threats may appear to remain outside the plant's longer-cycle learning and capability-building loop (e.g., institutionalized training coverage, multi-party exercises, and sustained reinforcement of preparedness for sabotage/terrorism scenarios). This imbalance suggests that continuity planning may still be more experience-driven. It is strengthened primarily through routine disruptions and familiar failure modes, rather than scenario-driven for rare but high-consequence intentional threats. A weaker signal is also visible for Natural Disasters under Adaptation (ND–A3), scored at 2.0, suggesting that revision and updating cycles for continuity arrangements may be less mature or less frequently exercised compared with stronger parts of the profile.

For Plant N, the heatmap shows a relatively even profile for supply chain disruption (SC), where all assessed capability cells are scored at 4.0, indicating consistent preparedness, continuity provisions, updating practices, and outcome signals within the assessed boundary. Human error (HE) also exhibits a strong longer-cycle signal, with HE–A4 scoring 5.0, suggesting well-institutionalized learning and embedding elements related to human-error prevention and reinforcement. In contrast, several disruption domains reveal pronounced fragile cells. The most notable is Technical Failures under Adaptation (TF–A3), scored at 1.0, indicating limited evidence of systematic updating or upgrading following technical-failure signals within the assessed boundary. Internal Labour Disruptions under Absorption (ILD–A2) is also scored at 1.0, suggesting limited capability to maintain safe and secure functioning during labour disruption conditions. Taken together, these disruption-level weak points provide concrete entry points for interpreting why Plant N's overall Adaptation capability (A3) is comparatively lower in the radar profile and motivate the targeted cross-case contrasts presented in Section 4.3.

5.4.2.3 Disruption-by-disruption baseline findings

To unpack the heatmap patterns (**Figure 5.3**), this subsection summarizes the baseline findings for each disruption domain by comparing (i) the capability pattern within each plant and (ii) the most salient cross-case contrasts. The intent is not to discuss every indicator individually, but to report dominant signals per disruption type while retaining traceability to the indicator set and the recorded evidence rationales. Where access conditions or N/A coverage differ, the interpretation relies on the recorded rationales rather than the numerical contrast alone.

Human Errors (HE). Plant M shows a balanced but less institutionalized profile, with weaker Anticipation (HE–A1 = 2.0), moderately strong Absorption (HE–A2 = 3.33), and moderate Ascension (HE–A4 = 3.5). Plant N shows a pronounced strength in Ascension (HE–A4 = 5.0), with moderate Anticipation and Absorption (HE–A1 = 2.5; HE–A2 = 3.0), indicating that learning and embedding signals are stronger than upstream readiness and continuity elements in the human-error domain. This contrast is consistent with evidence notes highlighting gaps in security-related human factors (e.g., security-awareness training described as “essentially non-existent”) for both plants, which constrains anticipation-oriented readiness within the human error domain.

Technical Failures (TF). Plant M exhibits a distinctly strong upstream and continuity posture (TF–A1 = 4.0; TF–A2 = 4.25) and a stronger Adaptation signal (TF–A3 = 3.0), indicating a more active improvement cycle after failures, while its Ascension score is lower (TF–A4 = 2.5). Meanwhile, Plant N shows solid continuity-oriented capacity and reasonable Ascension (TF–A2 = 3.75; TF–A4 = 3.5) but a very weak Adaptation signal (TF–A3 = 1.0), suggesting limited evidence of systematic updating or upgrading following technical-failure signals within the assessed boundary. This contrast aligns with evidence notes indicating that incidents were often followed by “repair in kind” and that upgrades were “seldom implemented after leaks,” which helps explain why adaptation appears constrained in the Plant N technical-failure profile.

Managerial Failures (MF). Plant M exhibits stronger Anticipation and higher Adaptation (MF–A1 = 4.0; MF–A3 = 3.67), but weaker Absorption and notably weaker Ascension (MF–A2 = 3.0; MF–A4 = 2.5). Plant N shows a comparatively stronger profile across Absorption and Ascension (MF–A2

= 4.0; MF–A4 = 4.0), with moderate Anticipation and Adaptation (MF–A1 = 3.5; MF–A3 = 3.0). Evidence notes suggest that part of this pattern is mediated by governance ownership: some security risk analysis functions were described as being handled externally at the industrial-park level, which limits plant-level ownership and visibility for certain security-related managerial-failure indicators and shapes what can be evidenced and embedded locally over time.

Internal Labour Disruptions (ILD). Plant M shows a more robust continuity posture (ILD–A2 = 4.0) while maintaining strong Ascension (ILD–A4 = 4.0). Plant N shows a sharp capability discontinuity: Anticipation and Ascension are relatively strong (ILD–A1 = 4.0; ILD–A4 = 4.0), but Absorption is very weak (ILD–A2 = 1.0), indicating limited capability to maintain safe and secure functioning under labour disruption conditions within the assessed scope. Adaptation (ILD–A3) is not assessable in either plant (NA), so cross-case interpretation focuses mainly on A2 as the defining contrast (Plant M > Plant N). This contrast is consistent with evidence notes describing that although automation exists, human intervention is still needed during process upsets, whereas under normal conditions "two shift engineers can run operations (without operators)," implying greater operational independence in Plant M during workforce disruptions.

Natural Disasters (ND). Plant M shows comparatively strong Absorption (ND–A2 = 4.0) but weaker Adaptation (ND–A3 = 2.0), indicating that short-term continuity arrangements are rated higher than revision and updating cycles for natural-disaster-related continuity planning within the assessed scope. Plant N shows moderate Absorption (ND–A2 = 3.0) but stronger Adaptation (ND–A3 = 3.0), suggesting a more mature updating/revision cycle for continuity arrangements in this domain. Both plants show similar outcome-layer positioning (ND–A4 = 3.0 in both cases). This pattern is consistent with evidence notes indicating that natural hazards were largely addressed through general emergency drills rather than dedicated natural-hazard scenario exercises, including the observation that flood-risk scenarios were not included, which limits institutionalized learning specific to natural hazards.

Terrorism/Sabotage (TS). Plant M shows a relatively complete profile with strong readiness and continuity (TS–A1 = 4.0; TS–A2 = 5.0; TS–A3 = 3.0) but a pronounced weakness in Ascension (TS–A4 = 1.0), indicating

limited longer-cycle institutionalization (e.g., training coverage and joint drills) for terrorism/sabotage scenarios. Plant N shows moderate scores where plant-level assessment was possible (TS–A1 = 3.5; TS–A2 = 4.0), but TS–A3 and TS–A4 are not assessable at plant level (NA). This creates an important boundary condition: the Plant N TS profile is mainly a readiness/continuity snapshot and does not extend into adaptation or longer-cycle embedding within the assessed scope. Evidence notes support the Plant M interpretation by stating that drills were conducted annually but mainly focused on fire or leakage emergencies and not on terrorism (unless framed as sabotage), suggesting why terrorism-specific learning and embedding signals remain weak.

Supply Chain Disruption (SCD). Plant M shows very strong upstream and operational posture (SCD–A1 = 5.0; SCD–A2 = 5.0; SCD–A3 = 5.0), but SCD–A4 is not assessable (NA), likely reflecting the nature of the result-type indicator and lack of justifiable disruption-history data for scoring. Plant N shows a consistently strong and even profile across all assessed capabilities (SCD–A1 = 4.0; SCD–A2 = 4.0; SCD–A3 = 4.0; SCD–A4 = 4.0), suggesting coherent supply resilience practices spanning readiness, continuity, improvement, and outcome-layer signals within the assessed boundary. This strong operational posture aligns with evidence that emphasizes the importance of effective inventory and supplier management for continuous operation, while also recognizing residual vulnerabilities, such as counterfeit-component risks for non-critical parts.

External Social Hazards (ESH). Plant M shows moderate readiness and continuity (ESH–A1 = 4.0; ESH–A2 = 4.0), with assessable Adaptation and stronger Ascension (ESH–A3 = 2.0; ESH–A4 = 4.0). Plant N shows strong readiness and continuity posture (ESH–A1 = 5.0; ESH–A2 = 5.0), but a low Ascension score (ESH–A4 = 2.0) and a non-assessable Adaptation cell (ESH–A3 = NA), indicating that while upstream arrangements for external social hazards are strong, the longer-cycle embedding/outcome layer is weaker or less evidenced within the assessed scope. This contrast aligns with the evidence note that the BCP developed for COVID-19 in 2020 was not reviewed, which is directly relevant to interpreting longer-cycle learning and institutionalization signals under external social hazards.

Summary of key disruption–capability signals.

Before examining indicator-type patterns, three salient disruption–capability combinations are highlighted for each plant based on the heatmap patterns and the disruption-level narrative. For Plant M, the strongest signals appear in supply chain readiness and continuity (SCD–A1 and SCD–A2, both 5.0) and in terrorism/sabotage continuity arrangements (TS–A2, 5.0), while the most critical fragility is the very low long-cycle capability for terrorism/sabotage (TS–A4, 1.0). For Plant N, the strongest signal is the long-cycle human error capability (HE–A4, 5.0), supported by strong upstream readiness and continuity for external social hazards (ESH–A1 and ESH–A2, both 5.0), while the most critical fragilities are the very low technical-failure adaptation signal (TF–A3, 1.0) and labour disruption continuity (ILD–A2, 1.0). These "top signals" provide a compact entry point to the profile and motivate the indicator-type interpretation presented next.

5.4.2.4 Indicator-type patterns

In addition to capability and disruption profiles, the baseline results were examined by indicator type (Management, Process, Result) using the Type tags embedded in the indicator catalogue. **Table 2** summarizes the distribution of indicators by type and the corresponding mean/median scores and N/A coverage for each plant (N/A excluded from aggregation).

Table 5.2: Indicator-type summary (Plant M vs Plant N)

Plant	Indicator type	n (total)	n (scored)	n (N/A)	N/A (%)	Mean score	Median score
Plant M	Management (M)	5	5	0	0.0	2.60	3.00
Plant M	Process (P)	41	38	3	7.3	3.53	4.00
Plant M	Result (R)	6	5	1	16.7	3.60	4.00
Plant N	Management (M)	5	4	1	20.0	3.50	3.50
Plant N	Process (P)	41	33	8	19.5	3.39	4.00
Plant N	Result (R)	6	6	0	0.0	3.33	3.50

Across the full indicator set (n = 52), Process indicators dominate the measurement structure (P = 41), while Management (M = 5) and Result

(R = 6) indicators are comparatively fewer. This composition matters for interpretation: the plant profiles are driven primarily by evidence of operational practices and routines (Process indicators), while Management and Result indicators provide a smaller set of higher-level governance and outcome signals.

For Plant M, Process indicators show a slightly stronger baseline (mean 3.53, median 4, n scored 38/41) than for Plant N (mean 3.39, median 4, n scored 33/41), consistent with the heatmap patterns where Plant M scores highly on continuity and protective-practice indicators (e.g., technical protection layers, maintenance and supply-chain routines). Plant M also exhibits a lower N/A rate for Process indicators (3/41; 7.3%) than Plant N (8/41; 19.5%), suggesting that operational evidence was more readily retrievable and/or more directly owned within the Plant M assessment boundary and workshop context. In Plant N, the higher N/A burden within Process indicators is consistent with bounded visibility and ownership of some practices (e.g., security-related arrangements coordinated at the industrial-complex level) and with indicators that could not be evidenced within the key-informant pathway.

Management indicators provide a more limited signal because this category contains only five indicators. Plant N's Management-indicator summary is higher (mean 3.50, median 3.5, *n* scored 4/5) than Plant M's (mean 2.60, median 3, *n* scored 5/5); however, this pattern should be read cautiously. It points to a possible area for further inquiry into governance and leadership arrangements, rather than a firm conclusion about institutionalized leadership readiness. One Management item in Plant N is also marked N/A (1/5; 20%), reflecting that certain governance or training arrangements may sit outside plant-level ownership or evidence visibility.

Result indicators also provide a limited but important outcome-oriented layer. In Plant N, all Result indicators were assessable (0/6 N/A) with a mean of 3.33 (median 3.5, n scored 6/6), whereas Plant M shows one Result indicator marked N/A (1/6; 16.7%) and a mean of 3.60 among scored items (median 4, n scored 5/6). Two practical constraints, visible in the evidence notes, shape interpretation: first, some Result items can be difficult to verify or quantify reliably (e.g., insurance premium changes or annual financial impact estimates), and second, some trend-based indicators are hard to justify when disruptions are rare or have not occurred within a

defensible reference period. Accordingly, Result indicators are presented as outcome signals that complement, rather than replace the practice-based insight from Process indicators, and their N/A patterns are treated as part of operationalization feasibility rather than as weak performance per se.

5.4.2.5 Not Applicable (N/A) data coverage

A practical feature of the RoPSS baseline profiles is that they preserve coverage information rather than forcing every indicator–cell to a score. In both plants, some indicators were marked N/A, and these markings are analytically meaningful because they distinguish between (i) genuinely weak capability signals and (ii) items that are not applicable, not owned within the assessed boundary, or not evidencable within the available timeframe and access conditions.

Consistent with the scoring protocol, N/A items were excluded from mean calculations; therefore, the capability- and disruption-level means should be interpreted alongside the N/A pattern as part of the baseline profile rather than as missingness to be "filled." Overall N/A coverage differs across cases: Plant N recorded 9/52 (17.3%) N/A items, while Plant M recorded 4/52 (7.7%). N/A concentration was highest in Plant N's Process indicators (8/41; 19.5%), compared with Plant M (3/41; 7.3%), indicating that a meaningful subset of practice-oriented measures could not be evidenced within Plant N's assessed boundary and access pathway. For this reason, cross-case numerical contrasts are interpreted together with N/A coverage and evidence rationales, rather than as direct like-for-like comparisons.

Across the dataset, N/A markings clustered into four recurring reasons. First, non-occurrence within the reference period: some indicators require an observable event to assess performance (e.g., response effectiveness following specific intrusion/tampering alerts) and were marked N/A where there were no relevant incidents during the period considered. Second, ownership or governance outside plant-level control: several indicators could not be assessed because the relevant arrangements were described as coordinated or owned externally (e.g., by an industrial-park-level security department), limiting site-user visibility into protocol review cycles, retraining practices, or closure of complex-level recommendations. Third, indicators not meaningful under local constraints: certain "best practice" formulations (e.g., multi-sourcing for critical parts) were treated as N/A where sourcing was legitimately constrained by the original equipment

manufacturer (OEM) requirements or reliability/quality assurance expectations, such that assigning a low score would misrepresent an intentional design choice rather than a vulnerability. Fourth, definitional overlap or redundancy within the local evidence structure: in Plant N, selected terrorism/sabotage drill-related items were marked N/A when they were considered duplicative of other assessed drill indicators, signalling a catalogue–context fit issue rather than weak performance.

Overall, N/A coverage should be read as an operationalization output in its own right. It makes the baseline profiles more interpretable by clarifying where "low" reflects capability gaps versus where assessment is limited by boundary conditions, applicability, or evidence traceability. This supports more disciplined cross-case interpretation and reinforces the need when using RoPSS in practice, to document ownership boundaries and evidence expectations alongside scores.

5.4.3 Cross-case contrasts

Building on the capability radar (**Figure 5.2**) and the disruption-by-capability heatmaps (**Figure 5.3**), cross-case contrasts were examined by comparing cell-level mean scores, excluding "N/A", and then interpreting the largest differences alongside the recorded evidence rationales and coverage information. Overall, the comparison suggests that the two plants exhibit different resilience emphases under the same RoPSS assessment structure. Plant M's baseline is strongest in short-cycle readiness and continuity (A1–A2), whereas Plant N's baseline is comparatively stronger in longer-cycle embedding (A4) but shows a weaker adaptation loop (A3) within the assessed boundary.

Several contrasts are concentrated in a small number of "fragile" or "strong" cells that are operationally meaningful because they point to specific capability gaps within particular disruption domains. The most pronounced Plant M advantage appears in Internal Labour Disruptions under Absorption (ILD–A2: Plant M = 4.0 vs Plant N = 1.0), and Technical Failures under Adaptation (TF–A3: Plant M = 3.0 vs Plant N = 1.0). In both cases, the evidence notes help explain why these cells separate: for ILD, Plant N's absorption was constrained by reliance on on-site human intervention during upsets, whereas Plant M's notes indicate a higher degree of operational independence under workforce constraints (e.g., limited staffing still enabling stable operation under normal disruption

conditions). For TF–A3, Plant N's adaptation signal was constrained by limited evidence of systematic upgrading following technical-failure signals, consistent with rationales indicating that post-incident actions may often remain "repair in kind," whereas Plant M's notes reflect a more explicit improvement cycle after failures within the assessed scope.

In contrast, Plant N's strongest relative signals cluster around longer-cycle institutionalization. This is most visible in Human Errors under Ascension (HE–A4: Plant N = 5.0 vs Plant M = 3.5) and Managerial Failures under Ascension (MF–A4: Plant N = 4.0 vs Plant M = 2.5). The Plant N rationales emphasise reinforcement and embedding mechanisms (e.g., retraining follow-up, tracking, and institutional learning routines), while Plant M notes indicate more modest or less consistently evidenced longer-cycle mechanisms in comparable domains. A further contrast appears for External Social Hazards under Ascension (ESH–A4: Plant M = 4.0 vs Plant N = 2.0), where Plant N evidence suggests that continuity arrangements developed during major external events (e.g., COVID-era BCP) were not consistently translated into sustained review and refresh routines.

Notably, several apparent contrasts are shaped by ownership boundaries and assessability constraints rather than performance gaps, which RoPSS makes explicit through "N/A" marking. This is most visible in Terrorism/Sabotage for Plant N, where TS–A3 and TS–A4 were not assessable at plant level (N/A), limiting the interpretable TS baseline to readiness and continuity (A1–A2). Evidence notes indicate that parts of the longer-cycle security function (e.g., protocol updates, retraining, or certain security studies) were owned externally at the industrial park level, reducing plant-level visibility. In Plant M, the clearest terrorism/sabotage signal is not an N/A boundary but a scored weakness in TS–A4 (1.0), linked to limited institutionalized training and drill coverage specific to terrorism/sabotage beyond general emergency drills. In Supply Chain (SC), the contrast is partly shaped by accessibility at the outcome layer. Plant N shows a complete and even profile across A1–A4 (all 4.0), whereas Plant M shows very strong A1–A3 (all 5.0) but SC–A4 is not assessable (N/A), consistent with result-type indicators being difficult to justify when disruption history is limited or trend-based claims cannot be evidenced.

Taken together, the cross-case contrasts demonstrate that RoPSS can generate comparable baseline profiles while retaining the contextual

information needed to interpret differences responsibly. The combination of cell-level contrasts, explicit N/A boundaries, and short evidence rationales provides an auditable basis for explaining why certain capabilities appear strong or weak within a given disruption domain, and whether that signal reflects a capability gap or an ownership and visibility constraint in industrial implementation.

5.4.4 Resilience-enhancing strategies

In addition to baseline scoring and profiling, RoPSS operationalization elicited resilience-enhancing strategies as qualitative Step 6 outputs. These strategies translate baseline diagnostic signals into practical improvement directions by specifying priority improvement areas and one key action expected within approximately three years. **Table 5.3** summarizes the Step 6 strategy outputs for Plant N and Plant M across the eight disruption domains.

Table 5.3: Key improvement areas and actions for enhancing the plant's resilience

Disruption type	Plant M key improvement areas and action	Plant N key improvement areas and action
Human Errors (HE)	**Areas:** strengthen competence and refresher training cycles; update procedures; simplify HMI and alarm logic. **Key action:** The plant will introduce a new auto-ignition procedure (HCl burner), run refresher training every two years, and add a clear pop-up alarm screen.	**Areas:** strengthen procedures and work instructions; improve training and drills; simplify and improve operator information (HMI/alarm logic). **Key action:** The plant will visualise major-hazard scenarios and explicitly clarify operator roles to prevent recurrence.
Technical Failures (TF)	**Areas:** strengthen maintenance standards and work instructions for critical jobs; improve spare-parts governance; strengthen reliability studies and follow-up (e.g., FMEA/RCM). **Key action:** The plant will upgrade critical spares governance (including obsolescence and OEM alignment), validate FMEA outputs, and create work instructions for all critical jobs.	**Areas:** strengthen preventive maintenance and condition monitoring; improve spare-parts management; strengthen reliability studies and follow-up (e.g., RCM/FMEA). **Key action:** The plant will improve spare-parts management as a priority reliability action.

Management Failures (MF)	**Areas:** strengthen hazard-analysis quality and cadence (PRA/HAZOP); strengthen contractor management; strengthen cross-functional engagement on governance issues. **Key action:** The plant will strengthen PRA/HAZOP and related follow-up, and improve contractor management practices in line with internal and regulatory expectations.	**Areas:** strengthen hazard/risk identification cadence (HazID/HAZOP/LOPA); improve governance visibility through KPIs/dashboards; strengthen follow-up on findings. **Key action:** The plant will complete HazIDs to clarify major-hazard risks and strengthen risk visibility.
Internal Labour Disruptions (ILD)	**Areas:** expand cross-training across functions; strengthen remote monitoring/control; reduce dependence on manual tasks through selective automation. **Key action:** The plant will implement cross-training through a six-month traineeship rotation and maintain engagement through dialogue sessions and staff satisfaction feedback.	**Areas:** strengthen labour–management communication; improve consultation mechanisms; improve communication channels (e.g., committees, digital boards). **Key action:** The plant will strengthen engagement with the works council in view of potential economic pressure and workforce disruption.
Natural Disasters (ND)	**Areas:** strengthen BCP and scenario coverage; strengthen flood and utility resilience arrangements; strengthen drills and recovery readiness. **Key action:** The plant will strengthen the Business Continuity Plan for natural disasters and expand emergency drill scenarios accordingly.	**Areas:** strengthen backup power and utilities resilience; strengthen communication network robustness; update business continuity arrangements. **Key action:** The plant will re-assess preparedness for backup power and utility failure scenarios.
Terrorism / Sabotage (TS)	**Areas:** strengthen incident-response protocols and joint drills; strengthen perimeter and detection measures; strengthen OT/ICS protections (segmentation/whitelisting) and access control. **Key action:** The plant will improve perimeter upkeep, implement multi-factor authentication, and migrate selected systems/applications from local servers to cloud infrastructure to improve security robustness.	**Areas:** strengthen access control; strengthen restricted-area management; strengthen identity assurance mechanisms (e.g., biometrics/MFA badges). **Key action:** The plant will restrict access to offices and warehouses to reduce exposure to intentional threats.

Supply Chain Disruptions (SCD)	**Areas:** strengthen supplier management and diversification; strengthen digital tracking and traceability; strengthen procurement capability (cross-training). **Key action:** The plant will implement digital supplier and inventory tracking (including QR-based inventory control), conduct cross-training/briefings, and complete the SAP HANA upgrade.	**Areas:** diversify suppliers for critical parts; increase buffer stock for key items; strengthen supply resilience planning. **Key action:** The plant will further diversify suppliers, focusing on critical parts.
External Social Hazards (ESH)	**Areas:** strengthen BCP review and refresh; strengthen stakeholder and community coordination; strengthen alternative logistics and service continuity arrangements. **Key action:** The plant will review and update all Business Continuity Plan procedures.	**Areas:** strengthen community engagement; strengthen utility backup agreements; strengthen pandemic/health-emergency preparedness. **Key action:** The plant will strengthen pandemic preparedness arrangements in case of future outbreaks.

Across both plants, the strategies cluster around three recurring levers. First, many proposals focus on strengthening procedures, competence assurance, and refresher training cycles, particularly in human error and emergency-related domains. Second, several strategies target stronger review and follow-up mechanisms, including more systematic hazard and risk identification activities and clearer tracking of actions. Third, both plants propose technology-enabled improvements to strengthen visibility and control, such as simplification of HMI and alarm logic, improved tracking and inventory systems, and strengthened access-control measures.

Plant M's strategies are mainly framed as plant-level implementation actions. They emphasize operational reinforcement through procedure updates and defined refresher cycles (HE), maintenance standards and work instructions for critical jobs with stronger spares governance (TF), digital traceability and ERP-related upgrades in procurement and stores (SC), and combined physical and cyber measures for intentional threats, including access-control strengthening, OT hardening, and improved incident-response readiness (TS). For natural disasters and external social hazards, Plant M's actions focus on strengthening and refreshing business continuity planning and drill scenario coverage.

Plant N's strategies show a more mixed profile across disruption domains, with a stronger emphasis on governance cadence, assurance mechanisms, and targeted control tightening in domains shaped by cross-boundary dependencies. Key actions include completing hazard identification studies to strengthen risk visibility (MF), tightening access to offices and warehouses (TS), supplier diversification for critical parts (SC), and re-assessment of backup power and utility-failure preparedness (ND). For external social hazards, Plant N highlights pandemic preparedness as the main improvement direction.

Taken together, the Step 6 outputs show that RoPSS supports not only baseline profiling but also structured translation of findings into actionable improvement directions. Plant M's strategy set is more strongly expressed through operational and systems-oriented actions within plant ownership, whereas Plant N's strategy set more often emphasizes assurance and governance mechanisms and targeted controls within a multi-actor industrial context.

5.5. Discussion

5.5.1 How RoPSS supports integrated process safety–security management in practice

This study asked how the RoPSS framework can be operationalized in chemical plant settings to support integrated management of process safety and process security. Ab Rahim et al. (2026) conceptualized RoPSS as a resilience engineering integration of safety and security, operationalized through a six-step management cycle and an indicator catalogue organized by disruption type, resilience capabilities (Anticipation, Absorption, Adaptation, Ascension) (Hollnagel, 2014; Woods, 2015), and indicator type (Management, Process, Result) (Meyer & Reniers, 2022). The present study advances that contribution by showing what this conceptual structure looks like when enacted in real plants: how the same organizing logic can be applied under contrasting industrial access and governance conditions, and what baseline outputs and implementation insights emerge from its practical use.

Across the two case studies, RoPSS was operationalized as a structured, semi-quantitative assessment and profiling process using the same disruption-organized instrument and scoring protocol. The approach

remained workable through (i) an embedded, cross-functional pathway (Plant M) and (ii) a bounded-access, key-informant pathway (Plant N), demonstrating transferability of the operational procedure despite different implementation constraints.

In both cases, operationalization generated three practically relevant outputs: (a) completed indicator scores accompanied by short evidence rationales and explicit "N/A" markings, (b) baseline resilience profiles summarized as capability-level patterns and disruption-by-capability heatmaps, and (c) candidate resilience-enhancing strategies elicited through the same structured reflection process.

The results indicate that RoPSS supports integrated process safety–security management primarily by providing a single organizing lens that keeps accidental and intentional disruption domains within one coherent assessment routine (C. Chen et al., 2019; G. Reniers et al., 2020). The disruption-by-disruption progression prevents the exercise from defaulting to safety-only hazards, while the capability framing provides a consistent way to discuss how readiness (Anticipation), continuity (Absorption), systematic updating (Adaptation), and longer-cycle reinforcement and improvement (Ascension) are supported across both safety and security concerns (Aven, 2019; Yang et al., 2023). This directly reflects the conceptual intent in Ab Rahim et al. (2026): integration is not achieved by collapsing safety and security into one metric, but by making their interactions visible through shared routines, infrastructures, and managerial processes that jointly shape resilience. In practice, the baseline profiles helped translate "integration" into specific signals within concrete disruption domains (e.g., fragile cells such as weak adaptation in technical-failure contexts or weak longer-cycle institutionalization for low-frequency intentional threats), thereby supporting prioritization and targeted follow-up.

A further practical insight, consistent with the systemic framing in Ab Rahim et al. (2026), is that integrated process safety–security capability is partly governed by ownership and accountability across organizational layers (Rasmussen, 1997a; Reason, 1997). RoPSS makes this visible by retaining coverage information through "N/A" markings and accompanying evidence notes, rather than forcing artificial numeric completeness. This distinction matters because a low score indicates a plausible capability

gap within the assessed boundary, whereas “N/A” often indicates non-applicability, limited evidence within the timeframe, or external ownership, for example, where security arrangements are coordinated at the corporate or industrial-park level. Preserving these boundary conditions improves interpretability and prevents misattribution, which is important for integrated safety–security management where responsibilities and evidence systems are frequently distributed.

Taken together, the two cases indicate that RoPSS can be operationalized as a feasible and transferable approach for integrated process safety–security sense-making. It provides a repeatable structure for eliciting, scoring, and documenting capability evidence across disruption types, while producing baseline profiles that are comparable across plants without stripping away the contextual information needed for responsible interpretation and action. In this way, the implementation evidence reported here complements Ab Rahim et al. (2026) by showing how the RoPSS concepts, particularly the 4As capability framing and the emphasis on Ascension as a distinct longer-cycle capability, function as practical organizing devices for integrated management in real chemical plant settings.

5.5.2 RoPSS as a mixed-method diagnostic and sense-making tool

A central premise in Chapter 4 is that integrating process safety and process security requires a resilience-oriented, socio-technical lens that can surface interactions across routines, infrastructures, and governance arrangements, rather than treating safety and security as parallel domains assessed in isolation. This perspective is also reflected in prior work on safety and security integration in major hazard settings (VTT, 2021; Ylönen et al., 2022). The present study shows that RoPSS operationalizes this premise by functioning as a diagnostic and sense-making tool (Weick & Sutcliffe, 2005). It produces structured baseline representations that support comparison and prioritization, while preserving the contextual explanations needed to interpret what the profiles mean in practice. This aligns with recent work showing how resilience-oriented tools can be implemented to generate profiles that support identification of strengths, weaknesses, and improvement priorities in safety management (Afonso-Fernandes et al., 2026).

First, RoPSS's semi-quantitative outputs (capability radar profiles and disruption-by-capability heatmaps) provide a clear comparative structure that makes patterns legible at multiple levels. Capability aggregation enables a rapid "big picture" view of whether a plant's baseline appears stronger in short-cycle capabilities (Anticipation and Absorption) or in longer-cycle capabilities (Adaptation and Ascension), while the disruption-level heatmaps identify where fragile cells concentrate within specific disruption domains. This aligns with the intent of the RoPSS indicator catalogue to provide an operational bridge between resilience concepts and measurable organizational practice through a structured set of indicators spanning disruption types and indicator categories (Ab Rahim et al., 2026). Importantly, the diagnostic value is not only in the numbers themselves but in how they guide attention: rather than attempting to represent "overall resilience" as a single score, RoPSS supports targeted inquiry into why particular disruption–capability combinations appear weaker and what kind of organizational change would plausibly strengthen them (Patriarca, Bergström, et al., 2018).

Second, the two cases reinforce RoPSS as a mixed-methods approach with a complementary quantitative and qualitative nature (Creswell, 2018). The semi-quantitative scoring provides structure, comparability, and aggregation, enabling the systematic derivation and comparison of performance scores, capability profiles, and heatmaps across plants and disruption domains. At the same time, these numerical representations alone cannot explain why some capabilities appear strong or weak. The qualitative component, captured through facilitated discussions and documented evidence notes (and, where applicable, interview-style elicitation), uncovers the rationales behind scores, reveals informal practices not fully captured by the indicators, and clarifies how organizational experience and context shape capabilities (including what is owned locally versus governed externally). This complementary logic strengthens interpretability and reduces the risk of treating the scores as stand-alone facts.

Third, RoPSS's diagnostic value is strengthened by making boundary conditions explicit, mainly where security-relevant arrangements are distributed across organizational levels (Schulman, 2020). Ab Rahim et al. (2026) emphasized governance-level resilience and the importance of learning and accountability loops that extend beyond immediate

operational response. In practice, this was reflected in the way "N/A" markings and evidence notes clarified when indicators could not be assessed due to external ownership, non-applicability, or limited evidence within the assessment window. Preserving these markings is not merely a data-handling decision; it becomes an operational insight about where responsibility, evidence systems, and follow-up mechanisms actually reside. This supports responsible sense-making by distinguishing between capability gaps that can be addressed within the plant and limitations that require coordination with site-level actors, corporate functions, or other stakeholders.

Finally, the diagnostic process elicited a structured reflection that supports improvement planning. Because participants were required to justify scores against anchors and to record brief rationales, the assessment naturally surfaced where existing arrangements were experience-driven, where updating cycles were weak or irregular, and where low-frequency/high-impact threats were less integrated into longer-cycle learning routines. This is particularly relevant to the conceptual motivation for including Ascension in Ab Rahim et al. (2026): the cases illustrate how organizations may sustain strong continuity through protection layers and routines, yet still exhibit gaps in institutionalized learning, training coverage, drill scope, and reinforcement mechanisms that would strengthen resilience over time (Hollnagel, 2006; Jain et al., 2020). In this sense, RoPSS functions not only as a profiling tool but also as a structured dialogue mechanism that links baseline patterns to plausible resilience-enhancing strategies, as reflected in the Step 6 outputs summarized in Section 4.4.



Overall, the findings indicate that RoPSS's practical value lies in combining (i) structured semi-quantitative profiling that supports comparison and prioritization, with (ii) qualitative rationales and boundary-aware coverage information that preserve interpretability and point to the organizational locus of action. This combination enables integrated process safety–security sense-making in a manner consistent with the theoretical framing in Ab Rahim et al. (2026), while remaining feasible under the access and governance constraints that characterize real-world chemical plant implementation (VTT, 2021).

5.5.3 Limitations and implications for use

This study is intentionally positioned as an operationalization and use case paper, and several limitations should be recognized when interpreting the baseline profiles. First, the evidence is derived from two case studies and is therefore context-dependent. The results demonstrate the feasibility and the nature of the outputs RoPSS can generate in realistic settings. Still, they should not be interpreted as benchmarking claims or generalizable performance statements beyond the two plants (Yin, 2017).

Second, the scoring approach is deliberative and semi-quantitative. Although indicator-specific anchors and recorded rationales reduce arbitrariness, the 1–5 ratings remain ordinal and depend on evidence availability and practitioner judgement. The baseline outputs are therefore best suited for diagnostic comparison and prioritization rather than fine-grained ranking or high-stakes accountability applications. In addition, "N/A" markings, while analytically meaningful, mean that aggregated means can be computed over different indicator subsets across plants, particularly where ownership and evidence-ability differ (e.g., security arrangements governed at corporate or industrial-park level). Numerical contrasts should therefore be interpreted together with coverage information and evidence notes.

Third, the implementation pathway influences what can be evidenced and whose perspectives are captured. The cross-functional workshop mode enabled broader representation of routines and evidence sources, whereas the bounded-access pathway concentrated interpretation through a key-informant channel shaped by confidentiality and multi-operator governance realities (VTT, 2021). These constraints are treated as empirical features of industrial implementation, but they affect confidence for certain disruption domains and indicator types, especially where controls, data, and follow-up loops are distributed across organizational layers.

Taken together, these limitations point to practical implications for use. RoPSS is most appropriately implemented as a facilitated diagnostic exercise that (i) defines boundaries and ownership explicitly before scoring, (ii) allocates time for structured deliberation rather than rapid "form-filling," and (iii) preserves an auditable trail of short evidence notes to support interpretation and follow-up. Under these conditions, the approach supports structured reflection and prioritization while remaining

transparent about what can and cannot be concluded within the assessed scope.

5.6. Conclusion

This chapter examined how the RoPSS framework can be operationalized in chemical plant settings to support integrated management of process safety and process security. The two case studies show that RoPSS can be enacted as a structured, semi-quantitative diagnostic assessment that remains workable under contrasting access and governance conditions, and that it can generate interpretable baseline profiles across both accidental and intentional disruption domains.

Three main conclusions emerge. First, RoPSS supports integration in practice by translating an abstract safety–security ambition into a repeatable assessment routine that makes capability patterns visible and supports prioritization. Second, the baseline results indicate that integrated resilience depends not only on protective capacity during disruptions, but also on how systematically organizations update practices and institutionalize learning for longer-cycle capability building, particularly in disruption domains that are low-frequency but high-consequence. Third, interpretability depends on transparency about evidence and scope. Preserving brief rationales and explicit coverage information helps distinguish plausible capability gaps from non-applicability or external ownership, which is especially important in multi-layer governance contexts where some security-related arrangements sit outside plant control.

In a broader context, this paper provides practice-based evidence on how a resilience-oriented process safety–security framework can be applied in real chemical plant settings without relying on probabilistic risk modelling or collapsing safety and security into a single metric. RoPSS is best viewed as a facilitated baseline tool for structured reflection, diagnostic sense-making and prioritization. It can also support translation of diagnostic findings into context-appropriate improvement actions. Future work should extend this operationalization evidence through longitudinal reassessment to examine capability change over time, and through broader stakeholder-based appraisal to examine adoption conditions and indicator relevance across sectors.

Chapter 6



Conclusion and Recommendations

Chapter 5 showed how the RoPSS framework can be operationalized in chemical plant settings to generate baseline resilience profiles, evidence rationales, and resilience-enhancing strategies. Having moved from literature review, to practitioner insights, to framework development, and finally to field application, the thesis now turns to synthesis. Chapter 6 brings together the findings from all preceding chapters in relation to the main and sub-research questions, discusses the theoretical and practical contributions of the thesis, reflects on methodological strengths and limitations, and presents recommendations for practice, policy, and future research.

6. CONCLUSION AND RECOMMENDATIONS

6.1 Key findings in relation to the research questions

This section synthesizes the main findings of the thesis in relation to the main research question and the four sub-research questions introduced in Chapter 1. It shows how the thesis progresses from identifying the fragmentation between process safety and process security risk management to developing and operationalizing the Resilience-oriented Process Safety and Process Security (RoPSS) framework for the chemical process industry (CPI).

As a whole, the findings indicate that integration requires more than the parallel application of existing methods. Instead, it calls for a resilience-oriented approach that recognizes the coupled nature of accidental and intentional disruptions, translates this understanding into a structured management framework, and supports practical application through measurable indicators and plant-level operationalization.

6.1.1 The resilience-oriented approach

The overarching question of this thesis is: ***How can process safety and process security risk management be integrated through a resilience-oriented framework for the chemical process industry?*** The overall finding of this thesis is that such integration can be achieved by treating process safety and process security not as separate management domains, but as interdependent parts of a shared socio-technical risk landscape, and by structuring their management through a resilience-oriented framework that links preparedness, continuity, adjustment, and long-term improvement. In this thesis, that integration is realized through the Resilience-oriented Process Safety and Process Security (RoPSS) framework, which organizes management around four resilience capabilities, namely Anticipation, Absorption, Adaptation, and Ascension, within a six-step management cycle.

The findings across the thesis indicate that resilience engineering provides an appropriate unifying logic for this integration because it shifts attention from isolated hazards or threats toward the broader question of how chemical plants maintain essential functions under both accidental and

intentional disruptions. This perspective is especially important in the CPI, where process safety and process security often interact through shared infrastructures, digital systems, organizational routines, and human activities. The thesis further shows that integration becomes more meaningful when resilience is not treated as an abstract concept, but translated into practical managerial steps and measurable indicators that can be used in real plant settings.

6.1.2 The fragmented methods

The first sub-research question asked: ***What does the existing literature reveal about methods for process safety, process security, and resilience in the chemical process industry, and their implications for integrated risk management?*** Using the PRISMA method for a systematic literature review, the findings of Chapter 2 show that the literature is methodologically rich but fragmented. Process safety methods are comparatively mature and supported by a wide range of established tools, whereas (process) security assessment and resilience assessment remain less consolidated. Although a number of methods show promise for capturing uncertainty, interdependencies, and sociotechnical complexity, most studies still treat process safety, process security, and resilience as separate or only partially connected domains.

The review also showed that semi-quantitative approaches occupy an important middle ground across the field. Meanwhile, systems-based methods such as Functional Resonance Analysis Method (FRAM), Process Resilience Analysis Framework (PRAF), Resilience-based Integrated Process Systems Hazard Analysis

(RIPSHA), and System-Theoretic Accident Model and Processes (STAMP) appear especially promising for more holistic analysis. However, the literature still lacks a coherent framework that genuinely integrates process safety, process security, and resilience within a single management approach for the CPI. This finding is important because it establishes the baseline intellectual gap addressed by the thesis. In other words, the need for integration is not simply assumed, but is clearly supported by the fragmented state of the existing literature.

6.1.3 The practitioner insights

The second sub-research question asked: ***How do practitioners perceive the integration of process safety and process security risk management through a resilience engineering lens?*** The semi-quantitative survey findings in Chapter 3 show that practitioners generally regard such integration as useful and beneficial. Of the 47 respondents, 72% considered integrating process safety and process security worthwhile, particularly because it may reduce operational redundancy, improve resource use, and enhance the comprehensiveness of risk management. Qualitative responses further indicated that practitioners often recognize that safety and security risks may arise from the same systems, infrastructures, and activities, even if the initiating causes differ in intentionality.

At the same time, the findings also show that practitioner support for integration is conditional rather than uncomplicated. Important barriers were identified, including lack of knowledge and awareness, insufficient resources, siloed communication, and limited coordination between safety and security functions. In addition, although respondents generally viewed resilience-oriented thinking positively, familiarity with resilience concepts was mostly slight to moderate, suggesting that resilience is not yet deeply embedded in routine practice. The findings, therefore, imply that resilience can serve as a promising lens for integration, but only if it is translated into practical language, organizational routines, and tools that practitioners can recognize and apply.

Another important finding from this chapter concerns the role of values and trade-offs. Practitioner responses showed that decision priorities shift depending on the scenario. In some situations, such as immediate personnel safety, process safety considerations dominate; in others, such as insider threats or access-related vulnerabilities, process security concerns become more prominent. This shows that integration is not merely a technical exercise, but also a matter of navigating competing objectives and organizational values.

6.1.4 The integrated framework

The third sub-research question asked: ***How can a resilience engineering paradigm be translated into an integrated risk management approach for process safety and process security in the chemical process industry?*** The answer provided by this thesis is the development

of the Resilience-oriented Process Safety and Process Security (RoPSS) framework. Findings from expert interviews and elicitation presented in Chapter 4 show that resilience engineering can be translated into an integrated risk management approach by organizing process safety and process security through four resilience capabilities, eight disruption categories, three performance indicator types, and embedding them within a six-step management cycle. This provides both a conceptual and managerial structure for integration.

A central finding is that process safety and process security should be understood as coupled socio-technical subsystems rather than parallel domains. From this perspective, the interaction between technical systems, digital infrastructures, organizational routines, and human behavior becomes central to integrated risk management. The RoPSS framework reflects this understanding by linking disruptions, system objectives, performance indicators, and improvement strategies across both safety and security.

Another key finding is the introduction of Ascension as a distinct resilience capability. Whereas many resilience formulations stop at restoration or recovery, this thesis argues that integrated risk management in the CPI also requires a forward-looking capability that consolidates recovery, learning, continuous improvement, and prevention. Ascension, therefore, extends the resilience logic of the framework beyond immediate restoration and connects operational experience with longer-term organizational and governance development. In this respect, the framework contributes not only to integration between safety and security but also to a more evolutionary understanding of resilience in the CPI.

6.1.5 The operationalization

The fourth sub-research question asked: ***How can a resilience-oriented framework be operationalized and applied in chemical plant settings?*** The findings of Chapter 5 show that RoPSS can be operationalized in practice as a structured semi-quantitative diagnostic and sense-making tool. Using the same disruption-organized instrument package in two contrasting case studies, the framework was applied to produce comparable outputs, including capability profiles, disruption-by-capability heatmaps, indicator-type summaries, and qualitative resilience-enhancing strategies. This demonstrates that the framework can function not only

as a conceptual model, but also as a practical instrument for plant-level reflection and improvement.

The case studies also show that operationalization does not require a single fixed implementation pathway. In Plant M, the application was supported by cross-functional workshop engagement and richer operational embedding. Meanwhile, in Plant N, it relied more heavily on iterative discussions under bounded access conditions. Despite these differences, both cases produced auditable baseline profiles. This suggests that RoPSS is flexible enough to be used under realistic industrial constraints, provided that scoring is evidence-informed, rationales are documented, and assessment boundaries are clearly defined.

A particularly important practical finding is that "N/A" indicators should be treated as meaningful operationalization outputs rather than as mere missing data. In the case studies, some indicators could not be assessed because they were outside plant-level ownership, not applicable within the local scope, or not evidencable within the available timeframe. Making these limits explicit improved the interpretability of the baseline profiles and helped distinguish between genuine capability gaps and assessment boundary conditions. This reinforces the idea that operationalization of integrated process safety-security resilience must remain sensitive to governance structures, access conditions, and evidence availability.

6.1.6 The overall synthesis

Taken together, the findings in relation to the research questions show a coherent progression across the thesis. First, the literature review established that existing methods remain fragmented across process safety, process security, and resilience. Second, the practitioner survey demonstrated that integration is seen as useful and important, but also revealed implementation barriers and the need to translate resilience into a more practical form. Third, the framework-development study transformed this need into the RoPSS framework, providing an integrated resilience-oriented structure for managing coupled safety-security risks. Fourth, the case studies demonstrated that the framework can be operationalized in real chemical plant settings to produce meaningful baseline resilience profiles and improvement directions.

Overall, the key findings of this thesis indicate that a more integrated approach to process safety and process security in the CPI is both well justified and feasible. A resilience-oriented approach that recognizes the socio-technical and governance nature of the CPI provides the basis for this integration. The RoPSS framework represents the thesis's response to this challenge by offering a structured way to diagnose, discuss, and strengthen integrated resilience across diverse disruption contexts.

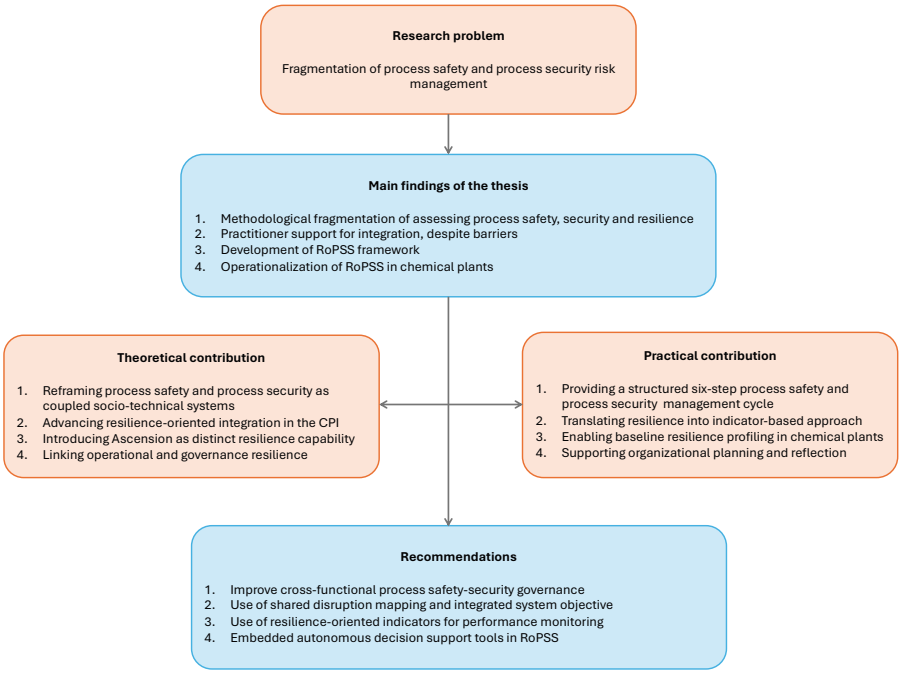

Figure 6.1 Overall research findings, contributions, and recommendations

Figure 6.1 summarizes the overall research findings, contributions, and recommendations of the thesis. It illustrates how the study progressed from addressing the fragmentation between process safety and process security risk management to generating four main findings: the methodological fragmentation in the literature, practitioner support for integration despite persistent barriers, the development of the RoPSS framework, and its operationalization in chemical plants. These findings underpin both the theoretical and practical contributions of the thesis and lead to several recommendations for practice and future research, which are elaborated in the subsequent sections.

6.2 Contributions of the thesis

Building on the key findings discussed in the previous section, this thesis makes several contributions to the integration of process safety and process security risk management in the CPI. These contributions are both theoretical and practical. At the theoretical level, the thesis advances the conceptual understanding of how process safety, process security, and resilience can be brought together within a unified socio-technical and governance perspective. At the practical level, it provides a structured framework and operational approach that can support organizational reflection, baseline resilience profiling, and improvement planning in chemical plant settings.

6.2.1 Theoretical contributions

This thesis makes several theoretical contributions to the body of knowledge on process safety, process security, resilience engineering, and integrated risk management in the CPI.

First, the thesis contributes by positioning process safety and process security as interdependent socio-technical subsystems within a shared major-hazard landscape, rather than as separate or parallel domains of management. While the literature has increasingly acknowledged interactions between safety and security, existing approaches often continue to treat them through separate methodological, regulatory, and organizational lenses. This thesis advances a more integrated understanding by showing that accidental and intentional disruptions may propagate through shared infrastructures, human activities, organizational processes, and digital systems. In this sense, the thesis shifts the analytical focus from managing isolated categories of risk toward understanding the coupled dynamics of safety and security within the same socio-technical system.

Second, the thesis contributes to resilience engineering by developing a resilience-oriented framework specifically tailored to the integration of process safety and process security in the CPI. Although resilience has gained increasing attention in major-hazard and critical-infrastructure research, it largely remains abstract or insufficiently translated into integrated management approaches for chemical process industries. This thesis extends that body of knowledge by showing how resilience can serve not merely as a general perspective on disruption, but as an organizing

paradigm for integrated process safety-security risk management. In doing so, the thesis connects resilience engineering more explicitly to the practical and organizational realities of the CPI.

Third, a key theoretical contribution of this thesis is the introduction of Ascension as a distinct resilience capability. Hollnagel's four cornerstones of resilience engineering describe resilient performance in terms of the abilities to anticipate, monitor, respond, and learn, while many applied resilience models characterize resilience through anticipation, absorption, adaptation, and restoration. The former emphasizes the core functions of resilient performance, whereas the latter reflects resilience across the disruption cycle. Building on both perspectives, this thesis argues that, in the context of integrated process safety and process security management, resilience should not stop at learning or restoration alone. Instead, it should also explicitly capture how recovery experience and lessons learned are translated into prevention, improved governance, continuous improvement, and stronger future performance. Ascension is proposed to capture this broader dimension. It therefore complements learning by emphasizing the institutionalization of lessons and extends restoration by moving beyond recovery toward the long-term strengthening of the system. In this respect, the thesis contributes a refined conceptualization of resilience that is particularly relevant for complex industrial systems exposed to recurring and emerging disruptions.

Fourth, the thesis contributes by linking operational resilience and governance resilience within a single framework. Much of the existing resilience literature focuses primarily on frontline performance, technical robustness, or immediate adaptive capacity. This thesis extends that focus by arguing that resilience in the CPI also depends on leadership, resource allocation, policy alignment, institutional learning, and cross-functional coordination. The RoPSS framework therefore conceptualizes resilience not only as a property of plant operations, but also as a governance function that shapes the conditions under which operational resilience can emerge and be sustained. This theoretical move is important because it broadens the meaning of integrated risk management beyond technical control and emergency response.

Fifth, the thesis contributes a structured conceptual architecture that links disruption types, resilience capabilities, and performance indicator

categories. Through the RoPSS framework, the thesis provides a systematic way of relating internal and external disruptions to the four resilience capabilities and to management, process, and result indicators. This architecture helps translate resilience from a broad theoretical notion into a more assessable logic for integrated risk management. It also provides a conceptual basis for understanding how different disruptions may challenge organizational performance in different ways and how these challenges can be interpreted across multiple dimensions of resilience.

Collectively, these theoretical contributions show that the thesis does more than propose a new framework for practice. It also advances the academic understanding of how process safety, process security, and resilience can be integrated conceptually within a common socio-technical and governance perspective.

6.2.2 Practical contributions

In addition to its theoretical value, this thesis makes several practical contributions to chemical plant management, industrial governance, and applied risk management in the CPI.

First, the thesis provides the RoPSS framework as a practical structure for integrated process safety and process security management. Rather than treating safety and security through separate routines, the framework offers a single management cycle through which organizations can define the system, identify disruptions, set system function objectives, select performance indicators, assess current performance, and formulate resilience-enhancing strategies. This gives practitioners a more coherent way of examining accidental and intentional risks together while preserving the distinct concerns of each domain.

Second, the thesis contributes a structured indicator-based approach that translates the framework into a practical tool for assessment and discussion. By organizing indicators according to disruption type, resilience capability, and indicator category, the thesis provides a means for plants to examine how their current arrangements support anticipation, absorption, adaptation, and ascension across a range of disruption contexts. This helps move integrated process safety-security management from a general aspiration to a more tangible organizational practice. It also allows the

framework to support baseline profiling, monitoring, and prioritization of improvement actions.

Third, the thesis demonstrates that the framework can be operationalized in real plant settings. The case studies show that RoPSS can be applied under contrasting implementation conditions, including both cross-functional workshop-based settings and more bounded-access, key-informant-led settings. This is an important practical contribution because real chemical plants often differ in their governance structures, evidence availability, access conditions, and resource constraints. The findings suggest that the framework is sufficiently flexible to support structured application across such differences, provided that assessment boundaries, evidence expectations, and rationale for scoring are explicitly documented.

Fourth, the thesis contributes a practical method for producing baseline resilience profiles that support organizational sense-making. Through capability radar charts, disruption-by-capability heatmaps, indicator-type summaries, and qualitative resilience-enhancing strategies, RoPSS enables plants to identify where strengths and weak points are concentrated. This is particularly useful for organizations seeking to understand not only whether they have safeguards in place, but also how their overall readiness, continuity, adaptation, and learning capacities vary across different disruption types.

Fifth, the thesis offers practical insight into the importance of ownership boundaries, evidence traceability, and non-assessable items in industrial assessment. The treatment of certain indicators as “N/A” in the case studies demonstrates that not every relevant function is always assessable within plant-level ownership or within the available evidence horizon. Making these boundaries explicit improves the interpretability of assessment results and avoids misleading conclusions. This is a practical lesson of broader relevance for resilience-oriented and integrated assessment approaches in complex industrial settings.

Sixth, the thesis provides practical guidance for improvement planning and organizational learning. The Step 6 resilience-enhancing strategies generated in the case studies show how baseline findings can be translated into concrete areas for action, such as strengthening training and competence assurance, improving review and follow-up

mechanisms, enhancing continuity arrangements, clarifying access control responsibilities, and reinforcing cross-functional communication. In this way, the thesis contributes not only a diagnostic tool, but also a structured basis for reflection and follow-up.

Finally, the practical relevance of the thesis extends beyond plant-level practitioners alone. The findings may also be useful for regulators, inspectors, policy actors, and industrial-complex coordinators who seek more integrated approaches to major-hazard governance. By highlighting the need to connect operational resilience with governance arrangements, and by making visible the interactions between safety, security, and organizational learning, the thesis offers practical value for a broader set of stakeholders involved in the prevention and management of major industrial disruptions.

Overall, the practical contributions of this thesis lie in its ability to provide a structured, usable, and context-sensitive approach for strengthening integrated resilience in the CPI. Rather than offering a final or universal assessment system, the thesis provides a practical foundation upon which organizations can build more coherent, reflective, and adaptive process safety and process security risk management practices.

6.3 Methodological reflections and limitations

This thesis adopted a multi-method research design to address a complex research problem that could not be adequately examined through a single method. The integration of process safety and process security through a resilience-oriented framework involves conceptual, empirical, and practical dimensions. It requires understanding the fragmented state of the literature, exploring practitioner perceptions, developing a coherent conceptual framework, and examining how that framework can be operationalized in real plant settings. For this reason, the combination of a systematic literature review, a mixed-methods practitioner survey, expert-informed framework development, and multiple case study applications provided an appropriate methodological pathway for the overall aims of the thesis.

A major strength of this research design lies in its sequential and cumulative logic. The systematic literature review established the conceptual and methodological fragmentation across process safety,

process security, and resilience assessment, thereby clarifying the need for a more integrated approach. The practitioner survey then added an empirical layer by showing that integration is generally viewed as useful, while also identifying important barriers, enabling factors, and value tensions that any proposed framework would need to address. Building on these foundations, the framework development study translated resilience engineering into the RoPSS framework through conceptual synthesis, expert interviews and elicitation, and indicator refinement. Finally, the case studies demonstrated how the framework could be operationalized in real plant settings and what kinds of diagnostic outputs it could produce in practice. In this sense, the thesis design supported a progression from problem diagnosis to conceptual response to practical application.

Another methodological strength of the thesis is that it combines breadth and depth in a complementary way. The literature review provided broad coverage of existing methods and debates. The survey offered wider practitioner perspectives across sectors and professional backgrounds. The expert interviews added depth and interpretive richness to the framework development stage, especially regarding resilience capabilities, integration challenges, and indicator design. The case studies then added contextual depth by showing how the framework behaved under actual organizational conditions, including differences in access, governance settings, and evidence availability. This layering of methods strengthened the credibility of the overall argument by ensuring that the thesis was informed by both academic knowledge and practical realities.

The methodology also reflects a deliberate effort to maintain relevance to practice. Rather than stopping at conceptual discussion, the thesis sought to ground the proposed framework in practitioner perceptions and expert-informed refinement, and to demonstrate its operational use in chemical plant settings. This practical orientation is important because resilience-oriented integration of process safety and process security cannot be meaningfully advanced if it remains disconnected from the language, constraints, and routines of industrial organizations. The case studies, in particular, showed that the framework could be applied under both embedded and bounded-access conditions, which increases confidence in its practical usability as a structured diagnostic and sense-making tool.

At the same time, several limitations should be acknowledged. First, the systematic literature review was bounded by specific inclusion and exclusion criteria. It focused on English-language journal articles published between 2000 and 2022 and excluded, among others, conference proceedings, book chapters, and studies outside the CPI or adjacent domains such as pure cybersecurity. These choices were appropriate for maintaining focus and comparability, but they also mean that the review may not have captured all relevant and most recent developments, especially practice-oriented or emerging work outside the selected corpus.

Second, the practitioner survey was exploratory in nature and based on a relatively small, non-random sample recruited through voluntary participation and snowball sampling. The sample was concentrated mainly in Malaysia and the Netherlands, and although it included respondents from industry, government, consultancy, and academia, it cannot be regarded as statistically representative of the wider CPI. In addition, the qualitative component of the survey relied on open-ended responses, which provided useful insights but did not offer the same depth and spontaneity as in-depth interviews. Nevertheless, the purpose of the survey was not statistical generalization, but rather to capture broad practitioner perceptions and implementation-relevant insights that could inform the subsequent framework development.

Third, the framework-development study should be interpreted as an expert-informed and formative stage rather than as conclusive validation. The RoPSS framework and its indicator catalogue were developed through conceptual synthesis, semi-structured expert interviews, scenario-based elicitation, and a focused importance–availability appraisal. These processes provided valuable grounding and refinement, but they do not establish that the framework is universally complete, final, or validated in a strong confirmatory sense. Rather, they show that the framework is theoretically informed, empirically supported through expert input, and sufficiently mature for practical operationalization and further testing. This distinction is important in order to calibrate the claims of the thesis appropriately.

Fourth, the case studies demonstrate operationalization and practical use, but they do not establish predictive validity, effectiveness outcomes, or broad generalizability across the CPI. The purpose of Chapter 5 was

to show how the framework can be applied, what kinds of baseline resilience profiles it can generate, and what implementation issues arise in practice. The two case studies, therefore, function as operationalization or use cases rather than validation cases in a strict sense. Moreover, the two plants differed in governance structure, access conditions, and evidence availability, which shaped the operationalization process and some of the scoring outcomes. Although this variation was analytically useful, it also means that the baseline profiles should be interpreted as context-dependent diagnostic outputs rather than as direct performance comparisons or universal benchmarks.

Fifth, the indicator-based assessment approach also has inherent limitations. The indicator set was intentionally designed as a semi-quantitative and practical tool, but some indicators required qualitative judgement, some depended heavily on local evidence availability, and some were marked as "N/A" because they were not assessable within plant-level ownership or the available timeframe. In addition, the aggregation approach used transparent unweighted averages in order to preserve interpretability, but this means that differential weighting of indicators and more advanced aggregation methods remain unresolved methodological questions. These limitations do not undermine the usefulness of the baseline profiling approach, but they do indicate that further refinement of the indicator system is both possible and desirable.

Despite these limitations, the overall methodology remains appropriate for the aims of the thesis. The chosen design enabled the research to move from conceptual fragmentation to practitioner insight, from framework development to field application, and from abstract resilience theory to a structured and operationally relevant approach for integrated process safety and process security risk management. The limitations, therefore, reflect not a weakness of the overall research logic, but the developmental stage of the work. They also point directly to the next steps required for broader empirical testing, methodological refinement, and future extension of the RoPSS framework.

6.4 Recommendations

The findings of this thesis point to several recommendations for both practice and future research. These recommendations follow directly from the identified integration gap, the practitioner insights, the development

of the RoPSS framework, and its operationalization in real plant settings. While the recommendations are presented separately for practice and research, they are closely related. Strengthening integrated process safety and process security management in the CPI requires both organizational action in the present and continued refinement of knowledge and tools in the future.

6.4.1 Recommendations for practice and policy

Firstly, chemical plant organizations should move beyond managing process safety and process security through largely separate routines and instead adopt more structured mechanisms for joint governance and coordination. The findings of this thesis show that fragmentation often persists through siloed responsibilities, limited communication, and different decision-making logics between safety and security functions. Organizations should therefore establish clearer cross-functional arrangements, such as integrated review platforms, shared responsibilities for interface issues, and more explicit mechanisms for joint decision-making in areas where safety and security overlap.

Secondly, organizations should strengthen the use of shared disruption mapping and integrated system objectives. Rather than assessing accidental and intentional risks through unrelated processes, plants should consider a broader set of internal and external disruptions within a common structure. This includes not only technical failures and human errors, but also managerial failures, labour disruptions, natural disasters, terrorism and sabotage, supply chain disruption, and external social hazards. Using a common disruption-based structure can help organizations recognize where process safety and process security are interdependent and where current arrangements leave blind spots.

Thirdly, chemical plants should incorporate resilience-oriented thinking more explicitly into existing management systems. This does not necessarily require replacing established process safety management systems or security programs. Rather, it means supplementing them with a perspective that asks how the organization anticipates, absorbs, adapts to, and improves after disruptions. In practice, this could involve using resilience capabilities as an organizing lens in workshops, audits, risk reviews, and management discussions. Such an approach can help shift

attention from isolated compliance tasks toward broader organizational capability and performance over time.

Fourthly, organizations should make greater use of integrated performance indicators to support reflection and improvement. The case studies demonstrated that an indicator-based baseline profile can help reveal strengths, weak points, and uneven capability development across disruption types. Plants should therefore consider using a concise and context-appropriate set of indicators that covers management, process, and result dimensions across both process safety and process security. The indicator system developed in this thesis may also serve as a basis for plant management and industry associations to develop their own tailored sets of indicators according to their specific operational context, governance arrangements, and priorities. At the same time, the findings also show that indicators should not be treated mechanically. Evidence traceability, boundary conditions, and ownership issues should be documented explicitly, and "N/A" outcomes should be recognized as meaningful information rather than as mere missing data.

Fifthly, management should invest more systematically in competence development, cross-training, and communication at the safety-security interface. The practitioner survey and expert interviews both highlighted lack of knowledge, limited awareness, and weak communication as major barriers to integration. Organizations should therefore strengthen training programs that expose personnel to both safety and security concerns, promote a shared vocabulary, and encourage joint problem-solving across disciplines. Cross-functional drills, workshops, and scenario-based discussions may be particularly useful in this respect, as they can reveal tensions and trade-offs before they emerge under real disruptive conditions.

A further recommendation is that organizations should place greater emphasis on longer-term learning and follow-up, not only on immediate recovery. One of the central arguments of this thesis is that resilience should not stop at restoring operations, but should also include the institutionalization of lessons, continuous improvement, prevention, and stronger governance. In practice, this means that post-incident reviews, drills, and assessments should not end with local corrective actions alone. They should also feed into updated procedures, revised training, stronger

coordination mechanisms, leadership attention, and more systematic reinforcement of preventive capacities over time.

Another recommendation concerns industrial governance and policy. Regulators, inspectors, and policymakers should encourage greater alignment between process safety and process security governance arrangements, especially in sectors where both accidental and intentional major-hazard risks are relevant. While the thesis does not argue for a complete merger of regulatory systems, it does suggest that stronger policy coordination, guidance on interface management, and recognition of resilience-oriented approaches could reduce the siloed treatment of these domains. This is particularly important for emerging and cross-domain issues, such as cyber-physical threats, complex industrial clusters, and disruptions that span organizational boundaries.

A related recommendation is that regulators and government agencies should give greater attention to natural-hazard-triggered technological accidents (NaTech) within integrated major-hazard governance. Natural hazards such as floods, storms, heatwaves, earthquakes, or lightning can compromise containment systems, utilities, access routes, emergency response capacity, and security arrangements at the same time. NaTech scenarios therefore illustrate the need for integrated and resilience-oriented oversight, because their consequences may cut across process safety, process security, emergency management, land-use planning, and critical infrastructure governance. Regulators could support this by encouraging operators to include NaTech scenarios in safety reports, emergency plans, business continuity arrangements, inspections, and joint exercises with relevant authorities. Such attention would help ensure that natural hazards are not treated only as external environmental events, but as potential initiators of major technological disruptions requiring coordinated preparedness, response, adaptation, and long-term learning.

Finally, for multi-operator industrial sites and industrial complexes, a specific recommendation is to clarify ownership boundaries and accountability for site-level versus plant-level functions. The case studies showed that some assessment difficulties arose not because plants performed poorly, but because relevant functions were governed externally or were only partly visible at plant level. Clearer governance arrangements regarding access control, emergency coordination, cybersecurity responsibilities, and

long-cycle follow-up would improve both practical management and the interpretability of resilience assessments.

6.4.2 Recommendations for future research

A first recommendation for future research is to apply the RoPSS framework in a broader range of chemical plant contexts and CPI subsectors. The present thesis demonstrates its operationalization in two chemical plant case studies, but wider application would help examine how the framework performs across different plant types, organizational structures, regulatory environments, and risk profiles. This would also support further refinement of the disruption categories, system objectives, and indicator interpretations.

A second recommendation is to investigate the framework longitudinally. In this thesis, RoPSS was used primarily to generate baseline resilience profiles. Future research should examine how these profiles evolve over time, how organizations respond to the identified weak points, and whether repeated application of the framework can support measurable improvement in integrated safety-security management. Longitudinal work would be especially useful in examining the practical significance of Ascension as a longer-term resilience capability.

A third recommendation is to continue refining the indicator system. Although the indicator catalogue developed in this thesis provides an operational foundation, future work should further examine issues such as indicator clarity, inter-rater consistency, context sensitivity, evidence requirements, and possible weighting or aggregation approaches. Such research would help strengthen the methodological robustness of the framework without losing its practical usability.

A fourth recommendation is to examine the RoPSS framework alongside established approaches such as STAMP, FRAM, and Bowtie analysis. Comparative studies of this kind could help clarify where RoPSS offers additional value, where it complements existing methods, and how its resilience-oriented and integration-focused features compare with more established approaches for managing coupled safety-security risks.

A fifth recommendation is to explore the relationship between RoPSS and autonomous decision-support tools. The framework currently operates

as a structured semi-quantitative and discussion-based approach, but future studies could investigate how digital dashboards, data integration systems, or software-supported scoring environments may support implementation, monitoring, and communication of resilience profiles. This may be especially valuable in larger facilities or industrial complexes where data ownership and coordination are distributed across multiple actors.

A sixth recommendation is to extend the framework's application to more explicit cyber-physical and cross-boundary contexts. The findings of this thesis suggest that the integration of process safety and process security becomes especially challenging where digital systems, shared infrastructures, contractor interfaces, and industrial-cluster governance arrangements intersect. Future work could therefore examine how RoPSS performs in settings where such interdependencies are more pronounced, and whether additional indicators or governance mechanisms are needed to address them more effectively.

A seventh recommendation is to examine the application of RoPSS to NaTech scenarios, where natural hazards trigger technological accidents or disrupt safety- and security-critical functions. Such work could explore how resilience capabilities, indicator requirements, and governance arrangements need to be adapted for hazards that cross organizational, infrastructural, and jurisdictional boundaries.

Another recommendation is to examine more closely the broader transferability of RoPSS beyond the CPI. Although the framework was developed and grounded in the CPI, its underlying socio-technical, resilience-oriented, and governance-based logic may also be relevant to other major-hazard and critical-infrastructure sectors in which safety and security are closely interconnected. However, such transfer should not be assumed. It requires empirical study and careful contextual adaptation of disruption categories, objectives, and indicators.

Finally, future research should examine the effectiveness and practical consequences of using RoPSS, not only its operationalization. The present thesis shows that the framework can be developed, refined, and applied in practice, but it does not yet establish whether its use leads to better organizational decisions, stronger resilience performance, or improved

integration outcomes over time. Addressing such questions would represent an important next step in the maturation of the framework.

6.5 Final conclusion

This thesis addressed the longstanding fragmentation between process safety and process security risk management in the chemical process industry. It showed that this separation limits organizations' ability to understand and manage accidental and intentional disruptions in an integrated way. In response, the thesis developed 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.

Through the development of the framework, its indicator architecture, and its application in two chemical plant case studies, the thesis has shown that a resilience-oriented approach can provide both a conceptual basis and a practical pathway for integration. In particular, the introduction of Ascension makes explicit the longer-term processes of recovery, learning, continuous improvement, prevention, and governance strengthening.

Overall, this thesis concludes that a more integrated approach to process safety and process security in the CPI is both well justified and practically feasible. More importantly, it shows that such integration should not be understood merely as the combination of two traditionally separate domains, but as a way of strengthening how organizations prepare for, respond to, adapt to, and improve after disruption. The true value of a resilience-oriented integration of process safety and process security lies not only in preventing harm, but in enabling organizations to endure disruptions, whether accidental or intentional, learn from them, and emerge stronger.

Appendix



References

Appendix A: Analysis of type, techniques, and stage of assessment

Appendix B: Balancing societal values

Appendix C: Full catalogue of resilience-oriented performance indicators

Appendix D: Context mapping headings and example observations

Appendix E: Operationalization artifacts and outputs

Appendix F: Online research dataset

Acknowledgements

Curriculum vitae

List of publications

References

Ab Rahim, M. S., Reniers, G., & Yang, M. (2024). Bridging Boundaries: Crafting a Resilient, Integrated Risk Management Model for Process Safety and Process Security. *Chemical Engineering Transactions* , *111*, 133–138. https://doi.org/10.3303/CET24111023

Ab Rahim, M. S., Reniers, G., & Yang, M. (2026). A resilience-oriented framework for managing process safety and process security. Process Safety and Environmental Protection, 215, 109182. https://doi.org/10.1016/j.psep.2026.109182

Ab Rahim, M. S., Reniers, G., Yang, M., & Bajpai, S. (2024). Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review. *Journal of Loss Prevention in the Process Industries*, *88*. 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

Adedigba, S. A., Khan, F., & Yang, M. (2017). Dynamic failure analysis of process systems using neural networks. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *111*, 529–543. https://doi.org/10.1016/j.psep.2017.08.005

Adedigba, S. A., Khan, F., & Yang, M. (2018). An integrated approach for dynamic economic risk assessment of process systems. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *116*, 312–323. https://doi.org/10.1016/j.psep.2018.01.013

Afonso-Fernandes, J., Barbosa, J., Arezes, P., Pardo-Ferreira, C., Rubio-Romero, J. C., & Rodrigues, M. A. (2026). Assessing resilience potentials in management of occupational safety and health in hospitals: Development and validation of a tool. *Journal of Safety Science and Resilience*, *7*(1). https://doi.org/10.1016/j.jnlssr.2025.100247

Alsulieman, A., Ge, X., Zeng, Z., Butenko, S., Khan, F., & El-Halwagi, M. (2024). Dynamic risk analysis of evolving scenarios in oil and gas separator. *Reliability Engineering and System Safety*, *243*. https://doi.org/10.1016/j.ress.2023.109834

American Chemistry Council. (2022). *2022 Guide to the Business of Chemistry*.

Amin, Md. T., Khan, F., Halim, S. Z., & Pistikopoulos, S. (2022). A holistic framework for process safety and security analysis. *COMPUTERS & CHEMICAL ENGINEERING*, *165*. https://doi.org/10.1016/j.compchemeng.2022.107963

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, *231*(3), 286–294. https://doi.org/10.1177/1748006X17699145

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

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

Aneziris, O. N., Papazoglou, I. A., Konstantinidou, M., & Nivolianitou, Z. (2014). Integrated risk assessment for LNG terminals. *Journal of Loss Prevention in the Process Industries*, *28*, 23–35. https://doi.org/10.1016/j.jlp.2013.07.014

API. (2021). *Process Safety Performance Indicators for the Refining and Petrochemical Industries*.

Argenti, F., Landucci, G., Cozzani, V., & Reniers, G. (2017). A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. *Safety Science*, *94*, 181–196. https://doi.org/10.1016/j.ssci.2016.11.022

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering and System Safety*, *92*(6), 745–754. https://doi.org/10.1016/j.ress.2006.03.008

Aven, T. (2017). How some types of risk assessments can support resilience analysis and management. *Reliability Engineering and System Safety*, *167*, 536–543. https://doi.org/10.1016/j.ress.2017.07.005

Aven, T. (2019). The Call for a Shift from Risk to Resilience: What Does it Mean? *Risk Analysis*, *39*(6), 1196–1203. https://doi.org/10.1111/risa.13247

Aven, T., & Kristensen, V. (2005). Perspectives on risk: Review and discussion of the basis for establishing a unified and holistic approach. In *Reliability Engineering and System Safety* (Vol. 90, Number 1, pp. 1–14). https://doi.org/10.1016/j.ress.2004.10.008

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

Ayyub, B. M. (2014). Systems resilience for multihazard environments: Definition, metrics, and valuation for decision making. *Risk Analysis*, *34*(2), 340–355. https://doi.org/10.1111/risa.12093

B, B., George, P., Renjith, V. R., & Kurian, A. J. (2020). Application of dynamic risk analysis in offshore drilling processes. *Journal of Loss Prevention in the Process Industries*, *68*. https://doi.org/10.1016/j.jlp.2020.104326

Bajpai, S., & Gupta, J. P. (2005). Site security for chemical process industries. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *18*(4–6), 301–309. https://doi.org/10.1016/j.jlp.2005.06.011

Bajpai, S., & Gupta, J. P. (2007). Terror-proofing chemical process industries. *Process Safety and Environmental Protection*, *85*(6 B), 559–565. https://doi.org/10.1205/psep06046

Bajpai, S., Sachdeva, A., & Gupta, J. P. (2010). Security risk assessment: Applying the concepts of fuzzy logic. *Journal of Hazardous Materials*, *173*(1–3), 258–264. https://doi.org/10.1016/j.jhazmat.2009.08.078

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

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

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

Baybutt, P. (2017a). Issues for security risk assessment in the process industries. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *49*, 509–518. https://doi.org/10.1016/j.jlp.2017.05.023

Baybutt, P. (2017b). Issues for security risk assessment in the process industries. *Journal of Loss Prevention in the Process Industries*, *49*, 509–518. https://doi.org/10.1016/j.jlp.2017.05.023

Benson, C., Argyropoulos, C. D., Dimopoulos, C., Mikellidou, C. V., & Boustras, G. (2021). Safety and risk analysis in digitalized process operations warning of possible deviating conditions in the process environment. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *149*, 750–757. https://doi.org/10.1016/j.psep.2021.02.0390957-5820/

Bevilacqua, M., Bottani, E., Ciarapica, F. E., Costantino, F., Di Donato, L., Ferraro, A., Mazzuto, G., Monteriu, A., Nardini, G., Ortenzi, M., Paroncini, M., Pirozzi, M., Prist, M., Quatrini, E., Tronci, M., & Vignali, G. (2020). Digital Twin Reference Model Development to Prevent Operators' Risk in Process Plants. *SUSTAINABILITY*, *12*(3). https://doi.org/10.3390/su12031088

Bischoff, H.-J., Sinay, J., & Vargová, S. (2015). Integrated Risk Management in Industries from the Standpoint of Safety and Security. *TRANSACTIONS of the VŠB – Technical University of Ostrava, Safety Engineering Series*, *9*(2), 1–7. https://doi.org/10.2478/tvsbses-2014-0005

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

Blokland, P., & Reniers, G. (2020). The Concepts of Risk, Safety, and Security: A Fundamental Exploration and Understanding of Similarities and Differences. In K. Bieder Corinne and Pettersen Gould (Ed.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (pp. 9–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_2

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Cameron, I., Mannan, S., Nemeth, E., Park, S., Pasman, H., Rogers, W., & Seligmann, B. (2017). Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better? *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *110*, 53–70. https://doi.org/10.1016/j.psep.2017.01.025

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

Casson Moreno, V., Garbetti, A. L., Leveneur, S., & Antonioni, G. (2019). A consequences-based approach for the selection of relevant accident scenarios in emerging technologies. *Safety Science*, *112*, 142–151. https://doi.org/10.1016/j.ssci.2018.10.024

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 Safety and Environmental Protection*, *116*, 621–631. https://doi.org/10.1016/j.psep.2018.03.026

Castillo-Borja, F., Vázquez-Román, R., Quiroz-Pérez, E., Díaz-Ovalle, C., & Sam Mannan, M. (2017). A resilience index for process safety analysis. *Journal of Loss Prevention in the Process Industries*, *50*, 184–189. https://doi.org/10.1016/j.jlp.2017.06.017

Castro Rodriguez, D. J., Barresi, A. A., & Demichela, M. (2025). "Resilience-based framework for enhancing NaTech risk management in industrial critical infrastructures." *Environment Systems and Decisions*, *45*(4). https://doi.org/10.1007/s10669-025-10056-9

CCPS. (2003). *Center for Chemical Process Safety (CCPS) Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* (1st Edition). John Wiley & Sons, Inc.

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.

Center for Chemical Process Safety. (2007). Guidelines for Risk Based Process Safety. In *American Institute of Chemical Engineers*. Wiley. https://doi.org/10.1002/9780470925119.fmatter

Chastain, J. W., Delanoy, P., Devlin, C., Mueller, T., & Study, K. (2017). Beyond HAZOP and LOPA: Four different company approaches. *Process Safety Progress*, *36*(1), 38–53. https://doi.org/10.1002/prs.11831

Chen, C., Li, J., Zhao, Y., Goerlandt, F., Reniers, G., & Yiliu, L. (2023). Resilience assessment and management: A review on contributions on process safety and environmental protection. *Process Safety and Environmental Protection*, *170*, 1039–1051. https://doi.org/10.1016/j.psep.2022.12.072

Chen, C., Reniers, G., & Khakzad, N. (2019). Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach. *Reliability Engineering and System Safety*, *191*. https://doi.org/10.1016/j.ress.2019.04.023

Chen, C., Yang, M., & Reniers, G. (2021). A dynamic stochastic methodology for quantifying HAZMAT storage resilience. *Reliability Engineering and System Safety*, *215*. https://doi.org/10.1016/j.ress.2021.107909

Chen, F., Wang, C., Wang, J., Zhi, Y., & Wang, Z. (2020). Risk assessment of chemical process considering dynamic probability of near misses based on Bayesian theory and event tree analysis. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *68*. https://doi.org/10.1016/j.jlp.2020.104280

Cheng, Y., Elsayed, E. A., & Huang, Z. (2022). Systems resilience assessments: a review, framework and metrics. *International Journal of Production Research*, *60*(2), 595–622. https://doi.org/10.1080/00207543.2021.1971789

Choi, J. Y., & Byeon, S. H. (2020). Hazop methodology based on the health, safety, and environment engineering. *International Journal of Environmental Research and Public Health*, *17*(9). https://doi.org/10.3390/ijerph17093236

Choi, J.-Y., & Byeon, S.-H. (2020). Hazop methodology based on the health, safety, and environment engineering. *International Journal of Environmental Research and Public Health*, *17*(9). https://doi.org/10.3390/ijerph17093236

Cong, G., Lu, D., Liu, M., Wang, Q., & Yu, W. (2021). A New Semi-Quantitative Process Safety Assessment Method and Its Application for Fluorochemical Industry. *PROCESSES*, *9*(10). https://doi.org/10.3390/pr9101695

Cox, L. A. (2008). Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. In *Risk Analysis* (Vol. 28, Number 6, pp. 1749–1761). https://doi.org/10.1111/j.1539-6924.2008.01142.x

Creswell. (2018). *Research Design - Qualitative, Quantitative, and Mixed Methods Approaches* (Fifth Edition). SAGE.

Dakkoune, A., Vernières-Hassimi, L., Leveneur, S., Lefebvre, D., & Estel, L. (2018). Risk analysis of French chemical industry. *Safety Science*, *105*, 77–85. https://doi.org/10.1016/j.ssci.2018.02.003

de Bruijn, H., & Herder, P. M. (2009). System and actor perspectives on sociotechnical systems. *IEEE Transactions on Systems, Man, and Cybernetics Part A:Systems and Humans*, *39*(5), 981–992. https://doi.org/10.1109/TSMCA.2009.2025452

Demichela, M., & Camuncoli, G. (2014). Risk based decision making. Discussion on two methodological milestones. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *28*, 101–108. https://doi.org/10.1016/j.jlp.2013.05.010

DHS, DOL, EPA, & OSHA. (2014). *Executive Order 13650 Actions to Improve Chemical Safety and Security – a Shared Commitment*. https://www.osha.gov/sites/default/files/final_chemical_eo_status_report.pdf

DOSH. (1996). *Occupational Safety and Health (Control of Industrial Major Accident Hazards) Regulations 1996*. Department of Occupational Safety and Health Malaysia. https://dosh.gov.my/wp-content/uploads/2024/10/Peraturan-Keselamatan-dan-Kesihatan-Pekerjaan-Kawalan-Terhadap-Bahaya-Kemalangan-Besar-Dalam-Perindustrian-1996.pdf

Dunbobbin, B. R., Medovich, T. J., Murphy, M. C., & Ramsey, A. L. (2004). Security vulnerability assessment in the chemical industry. *Process Safety Progress*, *23*(3), 214–220. https://doi.org/10.1002/prs.10037

El-Kady, A. H., Halim, S., El-Halwagi, M. M., & Khan, F. (2023). Analysis of Safety and Security Challenges and Opportunities Related to Cyber-physical Systems. *Process Safety and Environmental Protection*. https://doi.org/10.1016/j.psep.2023.03.012

Eskandarzade, M., Shahrivar, R., Ratnayake, R. M. C., & Bukhari, U. N. (2022). An Optimal Approach for Semiquantitative Risk-Based Inspection of Pipelines. *JOURNAL OF PIPELINE SYSTEMS ENGINEERING AND PRACTICE*, *13*(3). https://doi.org/10.1061/(ASCE)PS.1949-1204.0000653

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

European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). In *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555

Eva Magnusson, & Jeane Marecek. (2015). *Doing Interview-based Qualitative Research - A Learner's Guide*. Cambridge University Press.

Fang, J. N. S., Ford, D. M., & Mannan, M. S. (2004). Making the business case for process safety using value-at-risk concepts. *JOURNAL OF HAZARDOUS MATERIALS*, *115*(1–3), 17–26. https://doi.org/10.1016/j.jhazmat.2004.06.004

Fang, Y., Rasel, M. A. K., & Richmond, P. C. (2020). Consequence risk analysis using operating procedure event trees and dynamic simulation. *Journal of Loss Prevention in the Process Industries*, *67*. https://doi.org/10.1016/j.jlp.2020.104235

Flourish Studio. (2023). *https://app.flourish.studio/projects*.

Fouzi, N. F. R., Aziz, H. A., & Yaakub, N. (2024). Systematic review of chemical safety and chemical security risk management approach. In *Process Safety and Environmental Protection* (Vol. 183, pp. 676–686). Institution of Chemical Engineers. https://doi.org/10.1016/j.psep.2024.01.035

Geng, S., Yang, M., Mitici, M., & Liu, S. (2023). A resilience assessment framework for complex engineered systems using graphical evaluation and review technique (GERT). *Reliability Engineering and System Safety*, *236*. https://doi.org/10.1016/j.ress.2023.109298

Ghasemi, F., Gholamizadeh, K., Farjadnia, A., Sedighizadeh, A., & Kalatpour, O. (2022). Human and organizational failures analysis in process industries using FBN-HFACS model: Learning from a toxic gas leakage accident. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *78*. https://doi.org/10.1016/j.jlp.2022.104823

Glesner, C., Geysmans, R., & Turcanu, C. (2022). Two sides of the same coin? Exploring the relation between safety and security in high-risk organizations. *Journal of Safety Research*, *82*, 184–193. https://doi.org/10.1016/j.jsr.2022.05.010

Guo, C., Khan, F., & Imtiaz, S. (2018). Risk assessment of process system considering dependencies. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *55*, 204–212. https://doi.org/10.1016/j.jlp.2018.06.014

Guo, C., Khan, F., & Imtiaz, S. (2019). Copula-based Bayesian network model for process system risk assessment. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *123*, 317–326. https://doi.org/10.1016/j.psep.2019.01.022

Hansen, S. T., & Antonsen, S. (2024). Taking connectedness seriously. A research agenda for holistic safety and security risk governance. *Safety Science*, *173*. https://doi.org/10.1016/j.ssci.2024.106436

He, Z., Fu, M., & Weng, W. (2022). A non-linear risk assessment method for chemical clusters based on fuzzy measure and Choquet integral. *Journal of Loss Prevention in the Process Industries*, *77*. https://doi.org/10.1016/j.jlp.2022.104778

Hickford, A. J., Blainey, S. P., Ortega Hortelano, A., & Pant, R. (2018). Resilience engineering: theory and practice in interdependent infrastructure systems. *Environment Systems and Decisions*, *38*(3), 278–291. https://doi.org/10.1007/s10669-018-9707-4

Hollnagel, E. (2006). Resilience – the Challenge of the Unstable. In E. Hollnagel, David. D. Woods, & N. Leveson (Eds.), *Resilience Engineering: Concepts and Precepts* (1st Edition, pp. 9–17). CRC Press. https://doi.org/https://doi.org/10.1201/9781315605685

Hollnagel, E. (2014). *Safety-I and Safety-II: The Past and Future of Safety Management*. CRC Press.

Hollnagel, E. (2016). Resilience Engineering: A New Understanding of Safety. *Journal of the Ergonomics Society of Korea*, *35*(3), 185–191. https://doi.org/10.5143/jesk.2016.35.3.185

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016a). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety*, *145*, 47–61. https://doi.org/10.1016/j.ress.2015.08.006

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016b). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety*, *145*. https://doi.org/10.1016/j.ress.2015.08.006

HSE UK. (2006). *Developing process safety indicators : a step-by-step guide for chemical and major hazard industries*. Health and Safety Executive.

Hu, X., Wu, Z., Hedlund, F. H., Pedersen, J. B., Wang, R., Duo, Y., & Sin, G. (2018). Land-Use Planning Risk Estimates for a Chemical Industrial Park in China - A Longitudinal Study. *PROCESS SAFETY PROGRESS*, *37*(2), 124–133. https://doi.org/10.1002/prs.11972

Iaiani, M., Casson Moreno, V., Reniers, G., Tugnoli, A., & Cozzani, V. (2021). Analysis of events involving the intentional release of hazardous substances from industrial facilities. *Reliability Engineering and System Safety*, *212*. https://doi.org/10.1016/j.ress.2021.107593

ICCA. (2019). *The Global Chemical Industry: Catalyzing Growth and Addressing Our World's Sustainability Challenges Report for ICCA*.

ISO. (2019). *ISO 22301:2019 Security and resilience—Business continuity management systems—Requirements*. International Organization for Standardization (ISO).

ISO 31000: 2018. (2018). *ISO 31000:2018 Risk management - Guidelines*. https://www.iso.org/obp/ui/en/#iso:std:iso:31000:ed-2:v1:en

Jaeger, C. D. (2002). Vulnerability assessment methodology for chemical facilities (VAM-CF). *Chemical Health and Safety*, *9*(6), 15–19. https://doi.org/10.1016/S1074-9098(02)00389-1

Jahangiri, M., Zinat-Motlagh, K., Ghaem, H., Zinat-Motlagh, F., Kamalinia, M., & Banaee, S. (2021). Safety culture maturity and resilience engineering in an oil drilling industry: A comparison study among government-owned and private companies. *Work*, *70*(2), 443–453. https://doi.org/10.3233/WOR-213583

Jain, P., Diangelakis, N. A., Pistikopoulos, E. N., & Mannan, M. S. (2019). Process resilience based upset events prediction analysis: Application to a batch reactor. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *62*. https://doi.org/10.1016/j.jlp.2019.103957

Jain, P., Mentzer, R., & Mannan, M. S. (2018a). Resilience metrics for improved process-risk decision making: Survey, analysis and application. *Safety Science*, *108*, 13–28. https://doi.org/10.1016/j.ssci.2018.04.012

Jain, P., Mentzer, R., & Mannan, M. S. (2018b). Resilience metrics for improved process-risk decision making: Survey, analysis and application. *Safety Science*, *108*, 13–28. https://doi.org/10.1016/j.ssci.2018.04.012

Jain, P., Pasman, H. J., & Sam Mannan, M. (2020). Process system resilience: From risk management to business continuity and sustainability. *International Journal of Business Continuity and Risk Management*, *10*(1), 47–66. https://doi.org/10.1504/IJBCRM.2020.105615

Jain, P., Pasman, H. J., Waldram, S. P., Rogers, W. J., & Mannan, M. S. (2017). Did we learn about risk control since Seveso? Yes, we surely did, but is it enough? An historical brief and problem analysis. *Journal of Loss Prevention in the Process Industries*, *49*, 5–17. https://doi.org/10.1016/j.jlp.2016.09.023

Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E. N., & Mannan, M. S. (2018a). Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*, *53*, 61–73. https://doi.org/10.1016/j.jlp.2017.08.006

Jain, P., Pasman, H. J., Waldram, S., Pistikopoulos, E. N., & Mannan, M. S. (2018b). Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*, *53*. https://doi.org/10.1016/j.jlp.2017.08.006

Jain, P., Pistikopoulos, E. N., & Mannan, M. S. (2019). Process resilience analysis based data-driven maintenance optimization: application to cooling tower operations. *Computers and Chemical Engineering*, *121*, 27–45. https://doi.org/10.1016/j.compchemeng.2018.10.019

Jain, P., Rogers, W. J., Pasman, H. J., Keim, K. K., & Mannan, M. S. (2018c). A Resilience-based Integrated Process Systems Hazard Analysis (RIPSHA) approach: Part I plant system layer. *Process Safety and Environmental Protection*, *116*, 92–105. https://doi.org/10.1016/j.psep.2018.01.016

Jain, P., Rogers, W. J., Pasman, H. J., & Mannan, M. S. (2018d). A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer. *Process Safety and Environmental Protection*, *118*, 115–124. https://doi.org/10.1016/j.psep.2018.06.037

Jain, P., Rogers, W. J., Pasman, H. J., & Mannan, M. S. (2018e). A resilience-based integrated process systems hazard analysis (RIPSHA) approach: Part II management system layer. *Process Safety and Environmental Protection*, *118*, 115–124. https://doi.org/10.1016/j.psep.2018.06.037

Janošovský, J., Danko, M., & Labovský, J. (2019). Software approach to simulation-based hazard identification of complex industrial processes. *Computers and Chemical Engineering*, *122*, 66–79. https://doi.org/10.1016/j.compchemeng.2018.05.021

Jayaraman, S. N. B. F. R., Shariff, A. M., & Zaini, D. (2020). Stakeholder outreach on process safety for process industry using risk based approaches. *PROCESS SAFETY PROGRESS*, *39*. https://doi.org/10.1002/prs.12130

JCR. (2023). *Journal Citation Reports*. https://jcr.clarivate.com

Jianxing, Y., Haicheng, C., Shibo, W., & Haizhao, F. (2021). A Novel Risk Matrix Approach Based on Cloud Model for Risk Assessment Under Uncertainty. *IEEE ACCESS*, *9*, 27884–27896. https://doi.org/10.1109/ACCESS.2021.3058392

Jovanović, A., Øien, K., & Choudhary, A. (2018). An indicator-based approach to assessing resilience of smart critical infrastructures. In *Urban Book Series* (pp. 285–311). Springer. https://doi.org/10.1007/978-3-319-68606-6_17

Kamil, M. Z., Taleb-Berrouane, M., Khan, F., & Ahmed, S. (2019). Dynamic domino effect risk assessment using Petri-nets. *Process Safety and Environmental Protection*, *124*, 308–316. https://doi.org/10.1016/j.psep.2019.02.019

Kanes, R., Ramirez Marengo, M. C., Abdel-Moati, H., Cranefield, J., & Véchot, L. (2017). Developing a framework for dynamic risk assessment using Bayesian networks and reliability data. *Journal of Loss Prevention in the Process Industries*, *50*, 142–153. https://doi.org/10.1016/j.jlp.2017.09.011

Kannan, P., Flechas, T., Mendez, E., Angarita, L., Chaudhari, P., Hong, Y., & Mannan, M. S. (2016). A web-based collection and analysis of process safety incidents. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *44*, 171–192. https://doi.org/10.1016/j.jlp.2016.08.021

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 Safety Progress*, *29*(2), 133–143. https://doi.org/10.1002/prs.10354

Khan, F. I., & Abbasi, S. A. (2001). An assessment of the likehood of occurence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. *Journal of Loss Prevention in the Process Industries*, *14*(4), 283–306. https://doi.org/10.1016/S0950-4230(00)00048-6

Khan, F. I., Iqbal, A., & Abbasi, S. A. (2001). Rapid risk assessment of a fertilizer industry using recently developed computer-automated tool TORAP. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *14*(5), 413–427. https://doi.org/10.1016/S0950-4230(00)00055-3

Khan, F. I., Sadiq, R., & Husain, T. (2002). Risk-based process safety assessment and control measures design for offshore process facilities. *Journal of Hazardous Materials*, *94*(1), 1–36. https://doi.org/10.1016/S0304-3894(02)00004-3

Khan, F., Rathnayaka, S., & Ahmed, S. (2015). Methods and models in process safety and risk management: Past, present and future. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *98*, 116–147. https://doi.org/10.1016/j.psep.2015.07.005

Kim, K. H., Shin, D., & Yoon, E. S. (2003). Risk Analysis Using Automatically Synthesized Robust Accident Scenarios and Consequence Assessment for Chemical Processes: Process Partition and Consequence Analysis Approach. *Korean Journal of Chemical Engineering*, *20*(6), 992–999. https://doi.org/10.1007/BF02706927

Kleindorfer, P., Oktem, U. G., Pariyani, A., & Seider, W. D. (2012). Assessment of catastrophe risk and potential losses in industry. *COMPUTERS & CHEMICAL ENGINEERING*, *47*, 85–96. https://doi.org/10.1016/j.compchemeng.2012.06.033

Klockner, K., & Meredith, P. (2020). Measuring resilience potentials: A pilot program using the resilience assessment grid. *Safety*, *6*(4). https://doi.org/10.3390/safety6040051

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156–178. https://doi.org/10.1016/J.RESS.2015.02.008

Krishna, K., Wang, Y. J., Saraf, S. R., Rogers, W. J., Baldwin, J. T., Gupta, J. P., & Mannan, M. S. (2003). Hydroxylamine production: will a QRA help you decide? *RELIABILITY ENGINEERING & SYSTEM SAFETY*, *81*(2), 215–224. https://doi.org/10.1016/S0951-8320(03)00115-7

Ktori, R., Parada, M. P., Rodriguez-Pascual, M., van Loosdrecht, M. C. M., & Xevgenos, D. (2024). A value-sensitive approach for integrated seawater desalination and brine treatment. *Sustainable Production and Consumption*, *52*, 363–377. https://doi.org/10.1016/j.spc.2024.11.006

Landucci, G., Khakzad, N., & Genserik, R. (2020). *Physical Security in the Process Industry - Theory with Applications* (1st Edition). Elsevier B.V. https://doi.org/https://doi.org/10.1016/C2017-0-00539-6

Landucci, G., Khakzad, N., & Reniers, G. (2020). Physical security risk assessment tools and applications. In *Physical Security in the Process Industry* (pp. 71–123). Elsevier. https://doi.org/10.1016/b978-0-444-64054-3.00004-4

Lemley, J. R., Fthenakis, V. M., & Moskowitz, P. D. (2003). Security risk analysis for chemical process facilities. *Process Safety Progress*, *22*(3), 153–162. https://doi.org/10.1002/prs.680220304

Leveson, N. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press.

Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering and System Safety*, *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. In *SpringerBriefs in Applied Sciences and Technology* (pp. 17–27). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-47229-0_3

Leveson, N. G. (2011). Applying systems thinking to analyze and learn from events. *Safety Science*, *49*(1), 55–64. https://doi.org/10.1016/j.ssci.2009.12.021

Leveson, N. G., & Stephanopoulos, G. (2014). A system-theoretic, control-inspired view and approach to process safety. In *AIChE Journal* (Vol. 60, Number 1, pp. 2–14). https://doi.org/10.1002/aic.14278

Linkov, & Trump. (2019). *The Science and Practice of Resilience*. Springer. http://www.springer.com/series/13439

Logan, T. M. L., Aven, T., Guikema, S. D., & Flage, R. (2022). Risk science offers an integrated approach to resilience. In *Nature Sustainability* (Vol. 5, Number 9, pp. 741–748). Nature Research. https://doi.org/10.1038/s41893-022-00893-w

Mannan, S. (2012). *Lees' Loss Prevention in the Process Industries*. Elsevier.

Marhavilas, P. K., Filippidis, M., Koulinas, G. K., & Koulouriotis, D. E. (2019). The integration of HAZOP study with risk-matrix and the analytical-hierarchy process for identifying critical control-points and prioritizing risks in industry – A case study. *Journal of Loss Prevention in the Process Industries*, *62*. https://doi.org/10.1016/j.jlp.2019.103981

Marhavilas, P. K., Filippidis, M., Koulinas, G. K., & Koulouriotis, D. E. (2020). A HAZOP with MCDM based risk-assessment approach: Focusing on the deviations with economic/health/environmental impacts in a process industry. *Sustainability (Switzerland)*, *12*(3). https://doi.org/10.3390/su12030993

Marhavilas, P. K., Koulouriotis, D., & Gemeni, V. (2011). Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009. In *Journal of Loss Prevention in the Process Industries* (Vol. 24, Number 5, pp. 477–523). https://doi.org/10.1016/j.jlp.2011.03.004

Markowski, A. S. (2012). A review of layer of protection analysis techniques for oil and gas industry. *International Journal of Oil, Gas and Coal Technology*, *5*(1), 66–79. https://doi.org/10.1504/IJOGCT.2012.044178

Matteini, A., Argenti, F., Salzano, E., & Cozzani, V. (2019). A comparative analysis of security risk assessment methodologies for the chemical industry. *Reliability Engineering and System Safety*, *191*. https://doi.org/10.1016/j.ress.2018.03.001

Menezes, M. L. A., Haddad, A. N., & Nascimento, M. L. F. (2021). Functional Resonance Analysis Method and Human Performance Factors Identifying Critical Functions in Chemical Process Safety. *IEEE ACCESS*, *9*, 168368–168382. https://doi.org/10.1109/ACCESS.2021.3135747

Mentges, A., Halekotte, L., Schneider, M., Demmer, T., & Lichte, D. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. *International Journal of Disaster Risk Reduction*, *96*. https://doi.org/10.1016/j.ijdrr.2023.103893

Meyer, T., & Reniers, G. (2022). Risk management principles. In *Engineering Risk Management* (3rd Edition, pp. 43–109). De Gruyter.

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

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

Moore, D. A. (2013). Security risk assessment methodology for the petroleum and petrochemical industries. *Journal of Loss Prevention in the Process Industries*, *26*(6), 1685–1689. https://doi.org/10.1016/j.jlp.2013.10.012

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

Moreno, V. C., Marroni, G., & Landucci, G. (2022). Probabilistic assessment aimed at the evaluation of escalating scenarios in process facilities combining safety and security barriers. *RELIABILITY ENGINEERING & SYSTEM SAFETY*, *228*. https://doi.org/10.1016/j.ress.2022.108762

Myers, P. M. (2013). Layer of Protection Analysis - Quantifying human performance in initiating events and independent protection layers. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *26*(3), 534–546. https://doi.org/10.1016/j.jlp.2012.07.003

Necci, A., Cozzani, V., Spadoni, G., & Khan, F. (2015). Assessment of domino effect: State of the art and research Needs. *Reliability Engineering and System Safety*, *143*, 3–18. https://doi.org/10.1016/j.ress.2015.05.017

Nederlandse Arbeidinspectie. (2026). *Working Conditions Act (Arbowet)* . https://www.nllabourauthority.nl/topics/working-conditions-act

Nwankwo, C. D., Theophilus, S. C., & Arewa, A. O. (2020). A comparative analysis of process safety management (PSM) systems in the process industry. *Journal of Loss Prevention in the Process Industries*, *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

OPCW. (2021). *Indicative Guidelines for Chemical Safety and Security in Small and Medium-sized Enterprises to Foster the Peaceful Uses of Chemistry*.

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

Pasman, H. J., Knegtering, B., & Rogers, W. J. (2013). A holistic approach to control process safety risks: Possible ways forward. *Reliability Engineering and System Safety*, *117*, 21–29. https://doi.org/10.1016/j.ress.2013.03.010

Pasman, H. J., Rogers, W. J., & Mannan, M. S. (2018). How can we improve process hazard identification? What can accident investigation methods contribute and what other recent developments? A brief historical survey and a sketch of how to advance. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *55*, 80–106. https://doi.org/10.1016/j.jlp.2018.05.018

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

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

Pasman, H., & Rogers, W. (2014). How can we use the information provided by process safety performance indicators? Possibilities and limitations. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *30*, 197–206. https://doi.org/10.1016/j.jlp.2013.06.001

Pasman, H., & Rogers, W. (2015). The bumpy road to better risk control: A Tour d'Horizon of new concepts and ideas. *Journal of Loss Prevention in the Process Industries*, *35*, 366–376. https://doi.org/10.1016/j.jlp.2014.12.003

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. In *Safety Science* (Vol. 102, pp. 79–100). Elsevier B.V. https://doi.org/10.1016/j.ssci.2017.10.005

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

Patriarca, R., Di Gravio, G., Costantino, F., Falegnami, A., & Bilotta, F. (2018). An Analytic Framework to Assess Organizational Resilience. *Safety and Health at Work*, *9*(3), 265–276. https://doi.org/10.1016/j.shaw.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. *Journal of Loss Prevention in the Process Industries*, *69*. https://doi.org/10.1016/j.jlp.2020.104366

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

Perrow, C. (1999). *Normal Accidents: Living with High Risk Technologies - Updated Edition*. Princeton University Press.

Pettersen Gould, K., & Bieder, C. (2020a). Safety and Security: The Challenges of Bringing Them Together. In *SpringerBriefs in Applied Sciences and Technology* (pp. 1–8). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-030-47229-0_1

Pettersen Gould, K., & Bieder, C. (2020b). Safety and Security: The Challenges of Bringing Them Together. In K. Bieder Corinne and Pettersen Gould (Ed.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (pp. 1–8). Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_1

Pettersen, K. A., & Bjørnskau, T. (2015). Organizational contradictions between safety and security - Perceived challenges and ways of integrating critical infrastructure protection in civil aviation. *Safety Science*, *71*(PB), 167–177. https://doi.org/10.1016/j.ssci.2014.04.018

Podofillini, L., & Dang, V. N. (2012). Conventional and dynamic safety analysis: Comparison on a chemical batch reactor. *Reliability Engineering and System Safety*, *106*, 146–159. https://doi.org/10.1016/j.ress.2012.04.010

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

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

Rasmussen, J. (1997a). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Rasmussen, J. (1997b). Risk management in a dynamic society: a modelling problem. *Safety Science*, *27*(3), 183–213.

Raveendran, A., Renjith, V. R., & Madhu, G. (2022). A comprehensive review on dynamic risk analysis methodologies. *Journal of Loss Prevention in the Process Industries*, *76*. https://doi.org/10.1016/j.jlp.2022.104734

Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate Publishing Limited.

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. *Journal of Cleaner Production*, *19*(11), 1239–1249. https://doi.org/10.1016/j.jclepro.2011.03.002

Reniers, G. L. L. (2010). Multi-Plant Safety and Security Management in the Chemical and Process Industries. In *Multi-Plant Safety and Security Management in the Chemical and Process Industries*. https://doi.org/10.1002/9783527630356

Reniers, G. L. L., Dullaert, W., Audenaert, A., Ale, B. J. M., & Soudan, K. (2008). Managing domino effect-related security of industrial areas. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *21*(3), 336–343. https://doi.org/10.1016/j.jlp.2007.06.007

Reniers, G., Landucci, G., & Khakzad, N. (2020). What safety models and principles can be adapted and used in security science? *Journal of Loss Prevention in the Process Industries*, *64*. https://doi.org/10.1016/j.jlp.2020.104068

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

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

Roy, A., Srivastava, P., & Sinha, S. (2015). Dynamic failure assessment of an ammonia storage unit: A case study. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *94*, 385–401. https://doi.org/10.1016/j.psep.2014.09.004

Sano, K., Koshiba, Y., & Ohtani, H. (2020). Risk assessment and risk reduction of an acrylonitrile production plant. *JOURNAL OF LOSS PREVENTION IN THE PROCESS INDUSTRIES*, *63*. https://doi.org/10.1016/j.jlp.2019.104015

Santana, R., Vianna, S. S. V, & Silva, F. V. (2022). A novel approach in fuzzy bowtie analysis applying Takagi–Sugeno inference for risk assessment in chemical industry. *Journal of Loss Prevention in the Process Industries*, *80*. https://doi.org/10.1016/j.jlp.2022.104892

Schmitz, P., Reniers, G., & Swuste, P. (2021). Determining a realistic ranking of the most dangerous process equipment of the ammonia production process: A practical approach. *Journal of Loss Prevention in the Process Industries*, *70*. https://doi.org/10.1016/j.jlp.2021.104395

Schneller, L., Porter, C. N., & Wakefield, A. (2023). Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators. *Security Journal*, *36*(2), 333–349. https://doi.org/10.1057/s41284-022-00341-6

Schulman, P. R. (2020). Safety and Security: Managerial Tensions and Synergies. In K. Bieder Corinne and Pettersen Gould (Ed.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (pp. 87–95). Springer International Publishing. https://doi.org/10.1007/978-3-030-47229-0_9

Sivaraman, S., Tauseef, S. M., & Siddiqui, N. A. (2022). Investigative and probabilistic perspective of the accidental release of styrene: a case study in Vizag, India. *Process Safety and Environmental Protection*, *158*, 55–69. https://doi.org/10.1016/j.psep.2021.11.034

Smith, P., & Ragan, T. (1999). *Instructional Design* (2nd Edition). John Wiley & Sons, Inc.

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

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

Stantcheva, S. (2023). How to Run Surveys: A Guide to Creating Your Own Identifying Variation and Revealing the Invisible. *Annual Review of Economics*, (15), 205–234. https://doi.org/10.1146/annurev-economics

Sultana, S., Andersen, B. S., & Haugen, S. (2019). Identifying safety indicators for safety performance measurement using a system engineering approach. *Process Safety and Environmental Protection*, *128*, 107–120. https://doi.org/10.1016/j.psep.2019.05.047

Sun, H., Wang, H., Yang, M., & Reniers, G. (2022). A STAMP-based approach to quantitative resilience assessment of chemical process systems. *Reliability Engineering and System Safety*, *222*. https://doi.org/10.1016/j.ress.2022.108397

Sun, H., Yang, M., & Wang, H. (2022). A virtual experiment for measuring system resilience: A case of chemical process systems. *Reliability Engineering & System Safety*, *228*, 108829. https://doi.org/10.1016/J.RESS.2022.108829

Swuste, P., Theunissen, J., Schmitz, P., Reniers, G., & Blokland, P. (2016). Process safety indicators, a review of literature. *Journal of Loss Prevention in the Process Industries*, *40*. https://doi.org/10.1016/j.jlp.2015.12.020

Ta, G. C., Amir Sultan, M. M., Lee, K. E., Mokhtar, M., Tan, L. L., Omar, A. S., Omar, M. N., & Sulkafle, N. H. (2020). A Proposed Integrated Framework for Chemical Safety and Chemical Security. *Journal of Chemical Education*, *97*(7), 1769–1774. https://doi.org/10.1021/acs.jchemed.9b00999

Tong, Q., Yang, M., & Zinetullina, A. (2020a). A Dynamic Bayesian Network-based approach to Resilience Assessment of Engineered Systems. *Journal of Loss Prevention in the Process Industries*, *65*. https://doi.org/10.1016/j.jlp.2020.104152

Tong, Q., Yang, M., & Zinetullina, A. (2020b). A Dynamic Bayesian Network-based approach to Resilience Assessment of Engineered Systems. *Journal of Loss Prevention in the Process Industries*, *65*. https://doi.org/10.1016/j.jlp.2020.104152

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

van de Poel, I. (2021). Design for value change. *Ethics and Information Technology*, *23*(1), 27–31. https://doi.org/10.1007/s10676-018-9461-9

Varadharajan, S., & Bajpai, S. (2023). Chronicles of security risk assessment in process industries: Past, present and future perspectives. *Journal of Loss Prevention in the Process Industries*, *84*. https://doi.org/10.1016/j.jlp.2023.105096

Vaughen, B. K., Hurban, D. A., First, K., & Ness, A. (2020). The Risk Analysis Screening Tool: Part I, overview. *PROCESS SAFETY PROGRESS*, *39*(2). https://doi.org/10.1002/prs.12142

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

Vert, M., Sharpanskykh, A., & Curran, R. (2021). Adaptive resilience of complex safety-critical sociotechnical systems: Toward a unified conceptual framework and its formalization. *Sustainability (Switzerland)*, *13*(24). https://doi.org/10.3390/su132413915

Villa, V., Paltrinieri, N., Khan, F., & Cozzani, V. (2016). Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. *Safety Science*, *89*, 77–93. https://doi.org/10.1016/j.ssci.2016.06.002

VTT. (2021). *Integrated Management of Safety and Security Synergies in Seveso plants (SAF€RA 4STER) – Final report*.

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

Wang, H., Khan, F., Ahmed, S., & Imtiaz, S. (2016). Dynamic quantitative operational risk assessment of chemical processes. *CHEMICAL ENGINEERING SCIENCE*, *142*, 62–78. https://doi.org/10.1016/j.ces.2015.11.034

Wasileski, R. F., & Henselwood, F. (2011). LOPA onions: Peeling back the outer layers. *Process Safety Progress*, *30*(2), 122–125. https://doi.org/10.1002/prs.10427

Weick, K., & Sutcliffe, K. (2005). Organizing and the Process of Sensemaking. *Organization Science*, 409–421.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety*, *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 Safety and Environmental Protection*, *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. *Reliability Engineering & System Safety*, *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* (Vol. 6, pp. 591–629). Elsevier. https://doi.org/10.1016/bs.mcps.2022.05.002

Yin, R. K. (2017). *Case study research and applications: Design and methods* (Sixth edition). SAGE.

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. *Safety Science*, *151*. https://doi.org/10.1016/j.ssci.2022.105741

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

Yu, M., Quddus, N., Kravaris, C., & Mannan, M. S. (2020). Development of a FRAM-based framework to identify hazards in a complex system. *Journal of Loss Prevention in the Process Industries*, *63*, 103994. https://doi.org/10.1016/J.JLP.2019.103994

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. *Journal of Loss Prevention in the Process Industries*, *96*. https://doi.org/10.1016/j.jlp.2025.105632

Yuan, S., Yang, M., & Reniers, G. (2024). Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants. *Computers in Industry*, *155*. https://doi.org/10.1016/j.compind.2023.104056

Zairul, M. (2021). *Illustrasi Ringkas Analisa Tematik (AT) Menggunakan Perisian ATLAS.ti 8*. UPM Press.

Zarei, E., Ramavandi, B., Darabi, A. H., & Omidvar, M. (2021). A framework for resilience assessment in process systems using a fuzzy hybrid MCDM model. *Journal of Loss Prevention in the Process Industries*, *69*. https://doi.org/10.1016/j.jlp.2020.104375

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 Safety and Environmental Protection*, *199*. https://doi.org/10.1016/j.psep.2025.107319

Zhang, B., Liu, Y., & Qiao, S. (2019). A Quantitative Individual Risk Assessment Method in Process Facilities with Toxic Gas Release Hazards: A Combined Scenario Set and CFD Approach. *PROCESS SAFETY PROGRESS*, *38*(1), 52–60. https://doi.org/10.1002/prs.11979

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. *Chemical Engineering Research and Design*, *212*, 405–420. https://doi.org/10.1016/j.cherd.2024.10.036

Zhou, J., Reniers, G., & Zhang, L. (2019). Petri-net based attack time analysis in the context of chemical process security. *COMPUTERS & CHEMICAL ENGINEERING*, *130*. https://doi.org/10.1016/j.compchemeng.2019.106546

Zhou, S., Wang, Z., & Li, Q. (2022). A conceptual framework integrating numerical simulation with system theory based method for quantitative explosion process hazard analysis. *PROCESS SAFETY AND ENVIRONMENTAL PROTECTION*, *166*, 202–211. https://doi.org/10.1016/j.psep.2022.08.003

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

Zinetullina, A., Yang, M., Khakzad, N., Golman, B., & Li, X. (2021). Quantitative resilience assessment of chemical process systems using functional resonance analysis method and Dynamic Bayesian network. *Reliability Engineering and System Safety*, *205*. https://doi.org/10.1016/j.ress.2020.107232

Zio, E. (2018). The future of risk assessment. *Reliability Engineering and System Safety*, *177*, 176–190. https://doi.org/10.1016/j.ress.2018.04.020

Zotero. (2023). *https://www.zotero.org/user/login*.

Zou, P. X. W., Sunindijo, R. Y., & Dainty, A. R. J. (2014). A mixed methods research design for bridging the gap between research and practice in construction safety. *Safety Science*, *70*, 316–326. https://doi.org/10.1016/j.ssci.2014.07.005



A

Appendix A

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

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
1	(Bartolozzi et al., 2000)	Hazards and operability analysis (HAZOP) support tool	QL		x			x		
2	(Venkatasubramanian et al., 2000)	HAZOP-expert tool	SQ		x					
3	(F. I. Khan & Abbasi, 2001)	Quantitative domino effect analysis	QN		x		x	x	x	
4	(F. I. Khan et al., 2001)	Computer automated tool for risk assessment	SQ		x		x	x	x	
5	(Baybutt, 2002)	Matrix-based threat and process vulnerability analysis	QL	N		x	x	x	x	
6	(Caputo et al., 2002)	Fault tree analysis (FTA)	SQ		x		x	x	x	
7	(Jaeger, 2002)	Checklist-based vulnerability assessment methodology	QL			x	x	x	x	
8	(F. I. Khan et al., 2002)	Probabilistic FTA	QN		x		x	x	x	
9	(Kim et al., 2003)	Event tree analysis (ETA), Consequence analysis	SQ		x		x	x	x	
10	(Krishna et al., 2003)	Quantitative FTA	QN		x		x	x	x	
11	(Lemley et al., 2003)	Matrix-based security risk analysis	SQ	N						
12	(Dunbobbin et al., 2004)	Checklist-based security vulnerability assessment	QL	N		x	x	x	x	

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
13	(J. N. S. Fang et al., 2004)	Quantitative value-at-risk (VAR)	QN		x		x	x	x	
14	(Moorel, 2004)	Checklist-based security vulnerability assessment	QL	N		x	x		x	
15	(Renshaw, 2004)	Checklist, Quantitative Risk Assessment (QRA)	SQ		x		x	x	x	
16	(Bajpai & Gupta, 2005)	Matrix-based Security Risk Factor Table (SRFT)	QL			x	x	x	x	
17	(Moore, 2006)	Matrix-based Security Vulnerability Assessment (SVA)	QL			x	x		x	
18	(Bajpai & Gupta, 2007)	SRFT, Expert judgement	QL			x		x	x	
19	(Ramzan et al., 2007)	Extended HAZOP, ETA, Risk Matrix	SQ		x		x	x	x	
20	(G. L. L. Reniers et al., 2008)	Quantitative domino security risk assessment	QN			x		x		
21	(Bajpai et al., 2010)	SRFT, Expert judgement, Fuzzy logic	SQ			x		x	x	
22	(Wasileski & Henselwood, 2011)	LOPA	SQ		x		x	x	x	
23	(Kleindorfer et al., 2012)	Potential safety loss (near-miss) analysis	SQ		x		x	x	x	
24	(Markowski, 2012)	Fuzzy LOPA	SQ		x		x	x	x	
25	(Podofillini & Dang, 2012)	Monte Carlo probabilistic safety assessment	SQ		x		x	x	x	
26	(Ávila et al., 2013)	Social HAZOP	QL		x			x		
27	(Myers, 2013)	LOPA-based human performance	SQ		x		x			



No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
28	(Aneziris et al., 2014)	QRA	QN		x		x	x	x	
29	(Demichela & Camuncoli, 2014)	Extended HAZOP, dynamic ETA	SQ		x		x	x	x	
30	(Roy et al., 2014)	BN-based risk and reliability assessment	QN	N	x		x	x	x	
31	(Baksh et al., 2015)	BN-based predictive accident modeling	QN		x		x	x	x	
32	(Roy et al., 2015)	Dynamic BN-based, ETA	SQ				x	x	x	
33	(Wang et al., 2016)	Dynamic quantitative operational risk assessment	QN				x	x	x	
34	(Adedigba et al., 2017)	Artificial neural network (ANN), FTA, sequential accident model	SQ		x		x	x	x	
35	(Aneziris et al., 2017)	HAZOP, FTA and Bowtie	SQ		x		x	x	x	
36	(Argenti et al., 2017)	Quantitative SVA, Expert judgement	QN			x	x			
37	(Castillo-Borja et al., 2017)	Monte Carlo-based Safety Resilience Index	QN					x		x
38	(Chastain et al., 2017)	HAZOP, LOPA, Failure Mode and Effects Analysis (FMEA) Human Reliability Analysis (HRA)	SQ		x		x	x	x	
39	(Kanes et al., 2017)	BN, Bowtie	QN		x		x	x	x	
40	(Adedigba et al., 2018)	ETA, BN, modified inverted normal loss function	SQ		x		x	x	x	
41	(Dakkoune et al., 2018)	Risk Matrix	SQ		x		x	x	x	
42	(Guo et al., 2018)	Revised bow-tie with copula function and Monte Carlo simulation	SQ		x		x	x	x	

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
44	(Hu et al., 2018)	Simplified QRA	QN		x		x	x	x	
45	(Jain, Pasman, et al., 2018a)	Process resilience analysis framework (PRAF)	SQ		x		x	x	x	x
46	(Jain, Rogers, et al., 2018c)	HAZOP, Resilience-based integrated process systems hazard analysis (RIPSHA)	SQ		x		x	x	x	x
47	(Casson Moreno et al., 2019)	Bowtie and Consequence-based QRA	SQ		x		x	x	x	
48	(Guo et al., 2019)	BN-based Copula function	QN		x		x	x	x	
49	(Kamil et al., 2019)	Petri-net based dynamic domino effects risk assessment	SQ		x		x	x	x	
50	(J. Zhou et al., 2019)	Petri-net based attack tree analysis	QN			x	x	x	x	
51	(Jain, Diangelakis, et al., 2019)	PRAF with Bayesian analysis	QN		x		x	x	x	x
52	(Jain, Pistikopoulos, et al., 2019)	PRAF with Bayesian regression	QN		x		x	x	x	x
53	(Janošovský et al., 2019)	HAZOP, Aspen simulation	SQ		x			x		
54	(Marhavilas et al., 2019)	HAZOP, Risk Matrix, Analytical Hierarchy Process (AHP)	SQ		x		x	x	x	
55	(Song et al., 2019)	Dynamic BN-based Monte Carlo simulation, FTA	QN		x	x	x	x	x	
56	(Sultana et al., 2019)	System-Theoretic Accident Model and Processes (STAMP)	SQ		x			x	x	x

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
57	(Yousefi et al., 2019)	FRAM, STAMP, AcciMap	SQ		x			x	x	x
58	(B. Zhang et al., 2019)	QRA, Complete accident scenario set (CASS) and Computational fluid dynamics (CFD)	QN		x		x	x	x	
59	(B et al., 2020)	Dynamic BN-based, Bowtie	QN		x		x	x	x	
60	(Bjørnsen et al., 2020)	FRAM, Strength of Knowledge (SoK)	SQ		x			x	x	x
61	(F. Chen et al., 2020)	Dynamic BN-based ETA and Monte Carlo simulation	QN		x		x	x	x	
62	(H. Pasman et al., 2020b)	PRAF, RIPSHA	SQ	N	x		x	x	x	x
63	(J.-Y. Choi & Byeon, 2020)	HAZOP, Safety Integrity Level (SIL)	SQ		x		x	x	x	
64	(Marhavilas et al., 2020)	HAZOP, Risk Matrix, AHP	SQ		x		x	x	x	
65	(Sano et al., 2020)	Dow's Fire and Explosion Index (DFEI), FTA, Process Safety Metrics, Cost-benefit analysis (CBA)	QN		x		x	x	x	
66	(Tong et al., 2020b)	Dynamic BN, Markov Chain analysis	QN		x		x	x	x	x
67	(Vairo et al., 2020)	Dynamic BN-based and Markov Chain Monte Carlo	QN		x		x	x	x	x
68	(Y. Fang et al., 2020)	ETA-based, Aspen simulation	QN		x		x	x	x	
69	(Vaughen et al., 2020)	LOPA, Consequence modelling, Risk Matrix	SQ		x		x	x	x	
70	(Benson et al., 2021)	SIL	SQ	N	x		x	x	x	

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
71	(C. Chen et al., 2021)	Dynamic Monte carlo simulation, TNT explosion model, Probit model, Fire escalation model	QN		x		x	x	x	x
72	(Cong et al., 2021)	HAZOP, LOPA, Dow's Fire and Explosion Index (DFEI)	SQ		x		x	x	x	
73	(Jianxing et al., 2021)	Risk Matrix-based with fuzzy cloud model	SQ				x	x	x	
74	(Iaiani et al., 2021)	Correspondence Analysis (CA), Root Cause Analysis (RCA)	SQ			x		x	x	
75	(Menezes et al., 2021)	Functional Resonance Analysis Method (FRAM), Performance Shaping Factors (PSF)	QL		x			x	x	x
76	(Penelas & Pires, 2021)	HAZOP, Risk Matrix	QL		x			x	x	
77	(Schmitz et al., 2021)	Bow-tie, Phast simulation	SQ		x			x		
78	(Zarei et al., 2021)	Multicriteria decision-making (MCDM), AHP-VIKOR, Fuzzy set theory (FST)	SQ					x		x
79	(Zinetullina et al., 2021)	Dynamic BN, FRAM, Aspen HYSIS	SQ		x		x	x	x	x
80	(Amin et al., 2022)	BN-based integrated process safety and security analysis	QN		x	x	x	x	x	
81	(Eskandarzade et al., 2022)	API Risk Based Inspection Methodology, improved Kent Muhlbauer method	SQ				x	x	x	
82	(Ghasemi et al., 2022)	Fuzzy BN, Human Factors Analysis and Classification System (HFACS)	SQ		x		x	x	x	
83	(He et al., 2022)	BN-based, Fuzzy measure and Choquet integral	QN		x		x	x	x	

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
84	(Moreno et al., 2022)	Probabilistic SVA, ETA, FTA, Human reliability assessment (HRA)	QN		x	x	x	x	x	
85	(S. Zhou et al., 2022)	STAMP, Computational fluid dynamics (CFD), Convolutional neural network (CNN)	SQ		x		x	x	x	x
86	(Santana et al., 2022)	Bowtie, Python fuzzy sets, Takagi–Sugeno inference	SQ		x		x	x	x	
87	(Sivaraman et al., 2022)	FTA, Artificial Neural Network (ANN), human error assessment and reduction technique (HEART)	SQ		x		x	x	x	
88	(Sun, Yang, et al., 2022)	Dynamic BN, FRAM	QN					x		x
89	(Ylönen et al., 2022)	FTA, ETA, HAZOP, Content Analysis	SQ		x	x	x	x	x	

Notes:

Type refers to the nature of the method:

QL = Qualitative

QN = Quantitative

SQ = Semi-quantitative

Data?

Stage of Assessment as presented in the study:

Safe. HI = Process safety-related hazard identification

Sec. HI = Process security-related hazard identification

LA = Likelihood and/or vulnerability analysis

CA = Consequence of event analysis

RC = Overall risk calculation

No.	Reference (Chronological ordered)	Techniques / Tools	Type	Data?	Stage of Assessment					
					Safe. HI	Sec. HI	LA	CA	RC	Res.
	N = No empirical or simulation data				Res. = Resilience assessment					
	presented in the study									

Appendix B

Balancing societal values within process safety and process security.

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

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

Scenario 1: Evacuation vs. Lockdown

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

Scenario 2: Unexpected Chemical Leak During Transport

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

Scenario 3: Insider Threat

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

Scenario 4: Conflicting Design Requirements

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

Scenario 5: Transparency with Regulatory Bodies

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



Appendix C

Full Catalogue of Resilience-Oriented Performance Indicators

This appendix provides the complete catalogue of resilience-oriented performance indicators developed as part of the Resilience-oriented Process Safety and Process Security (RoPSS) framework. The catalogue covers all eight disruption types identified in this study: human errors, technical failures, managerial failures, internal labor disruptions, natural disasters, terrorism/ sabotage, supply chain disruptions, and external social hazards. It is structured across the four resilience capabilities (anticipation, absorption, adaptation, and ascension). Indicators are further organized into three functional categories: management, process, and result indicators.

Each indicator is presented together with its five-point scale, allowing for consistent assessment across organizations. Depending on the nature of the indicator, the scale may be expressed quantitatively (e.g., percentage achievement), semi-quantitatively (e.g., frequency or ratio), or qualitatively (e.g., evidence of reviews or implementation). These scales provide a standardized basis for monitoring, benchmarking, and continuous improvement, while allowing flexibility for application in different organizational contexts.

Notes:
Dis. = Disruption category; Cap. = Resilience capability; Type = Indicator type;
HE = Human errors; TF = Technical failures; MF = Managerial failures; LD = Internal labor disruptions;
ND = Natural disasters; TS = Terrorist/ Sabotage; SC = Supply chain disruptions; SH = External social hazards;
A1 = Anticipation; A2 = Absorption; A3 = Adaptation; A4 = Ascension;
M = Management indicator; P = Process indicator; R = Result indicator.

Code	Dis.	Cap.	Type	Indicator
PI-01	HE	A1	M	During annual assessments, to what extent do operators demonstrate competence (skills, rules, and knowledge) to manage routine operations and unexpected incidents (for example, by applying process safety protocols)? *Scale:* *1. Operators struggle with basic process safety measures and require close supervision to avoid unsafe actions.* *2. Operators follow some standard procedures but have limited ability to address non-routine safety issues, indicating gaps in deeper safety knowledge.* *3. Operators adequately apply core safety protocols and can handle some unexpected events, but still need guidance for complex or evolving situations.* *4. Operators consistently adhere to safety rules, demonstrating strong skills in routine operations and effective problem-solving when unforeseen incidents arise.* *5. Operators excel at identifying and mitigating potential safety hazards, applying both procedural and knowledge-based approaches with minimal oversight, even under novel or high-stress conditions.*
PI-02	HE	A1	P	The overall percentage of employees who have attended security awareness sessions in the last 5 years. *Scale:* *1. Very Low Coverage: < 25% attendance or participation.* *2. Low Coverage: 25 – 49% attendance or participation.* *3. Moderate Coverage: 50 – 74% attendance or participation.* *4. High Coverage: 75 – 89% attendance or participation.* *5. Very High Coverage: ≥ 90% attendance or participation.*

Code	Dis.	Cap.	Type	Indicator
PI-03	HE	A2	P	During demand events caused by human error (e.g., misoperation, skipped step), how often are automatic safety barriers or interlocks activated and successfully prevent escalation to a major incident? *Scale:* *1. Unreliable: More than two in ten demands fail (< 80 %).* *2. Marginal: Eight in ten demands for activation are successful (80 – 89 %).* *3. Adequate: Nine in ten demands activation succeed (90 – 94 %).* *4. Robust: The barrier performs on virtually every demand (95 – 99 %).* *5. Highest integrity: No recorded activation failures (100 %).*
PI-04	HE	A2	R	How often do human error demands occur that lead to the use of a safety instrumented system (SIS) per year on average? *Scale:* *1. Very High Demand: > 100 % of the demand rate assumed in the SIL/LOPA study* *2. High Demand: 51 – 100 % of the design demand rate* *3. Moderate Demand: 26 – 50 % of the design demand rate* *4. Low Demand: 11 – 25 % of the design demand rate* *5. Very Low Demand: ≤ 10 % of the design demand rate*
PI-05	HE	A2	P	To what extent are dual-verification safeguards within the company in place and correctly applied for critical security actions (e.g., SIS bypass, hazardous-storage access, parameter control-system changes) that could escalate into a major incident? *Scale:* *1. Absent: No dual-verification requirement exists for critical actions.* *2. Minimal implementation: < 50 % of critical actions are dual-verified.* *3. Partial implementation: 50 – 79 % of critical actions are dual-verified.* *4. High implementation: 80 – 99 % of critical actions are dual-verified.* *5. Fully implemented: 100 % of critical actions are dual-verified.*

Code	Dis.	Cap.	Type	Indicator
PI-06	HE	A2	P	Over the past 12 months, how efficiently/ quickly were the responses to intrusion or tampering alerts (e.g., fence-line breach, badge-denied tailgating, SIS logic-change attempt) successfully / adequately detected and responded to? *Scale:* *1. Unreliable: It took more than two hours to successfully respond to a security breach.* *2. Marginal: It took 1 - 2 hours to successfully respond to a security breach.* *3. Adequate: It took 31 - 60 minutes to successfully respond to a security breach.* *4. Robust: It took 11 - 30 minutes to successfully respond to a security breach.* *5. Highest security: It took 0 - 10 minutes to successfully respond to a security breach.*
PI-07	HE	A3	P	After an incident highlights a procedural or training gap, how quickly are the affected safety/security procedures usually reviewed and updated? *Scale:* *1. Very slow: Less than half of the related procedures are updated within a year after the investigation report.* *2. Slow: Over half of the related procedures are updated within a year after the investigation report.* *3. Moderate: All the related procedures are updated within a year after the investigation report.* *4. Fast: All the related procedures are reviewed and updated in 1 – 6 months after the investigation report.* *5. Very fast: All the related procedures and protocols are reviewed and updated within a month after the investigation report.*
PI-08	HE	A4	P	Last year, to what extent were lessons from human-error incidents integrated into daily operations (e.g., updated procedures, training, human-machine interface (HMI), or policies)? *Scale:* *1. Very Low Coverage: Very few lessons are integrated into daily operations or policies.* *2. Low Coverage: Fewer than half of the lessons are integrated into daily operations or policies.* *3. Moderate Coverage: More than half of the lessons are integrated into daily operations or policies.* *4. High Coverage: Almost all lessons are integrated into daily operations or policies.* *5. Very High Coverage: All lessons are integrated into daily operations or policies.*

Code	Dis.	Cap.	Type	Indicator
PI-09	HE	A4	P	After a safety/security procedure update, to what extent have operators whose tasks are affected been notified and trained with the updated procedure? *Scale:* *1. A part of the operators have received training after two years about the updated procedure.* *2. A part of the operators have received training within two years about the updated procedure.* *3. A part of the operators have received training within one year about the updated procedure.* *4. All operators have received training within two years on the updated procedure.* *5. All operators have received training within one year on the updated procedure.*
PI-10	TF	A1	M	Proportion of the annual budget allocated for scheduled preventive maintenance of (critical) equipment to the total budget required for full maintenance coverage. *Scale:* *1. A small fraction (< 25%) of the maintenance budget is allocated for preventive maintenance.* *2. Less than half (25–49%) of the maintenance budget is allocated for preventive maintenance.* *3. More than half (50–74%) of the maintenance budget is allocated for preventive maintenance.* *4. Most (75–89%) of the maintenance budget is allocated for preventive maintenance.* *5. Almost all (≥ 90%) of the maintenance budget is allocated for preventive maintenance.*
PI-11	TF	A1	P	Proportion of unplanned vs. planned maintenance works over the last 12 months. *Scale:* *1. Very Reactive: > 75 % of all work orders are unplanned/ break-in/ emergency basis.* *2. Reactive: 50 – 74 % of all work orders are unplanned/ break-in/ emergency basis.* *3. Moderate: 25 – 49 % of all work orders are unplanned/ break-in/ emergency basis.* *4. Proactive: 10 – 24 % of all work orders are unplanned/ break-in/ emergency basis.* *5. Very Proactive: Virtually all (≤ 10 %) work is planned; unplanned or emergency work is rare.*

Code	Dis.	Cap.	Type	Indicator
PI-12	TF	A1	P	To what extent are rotating equipment capable of releasing hazardous fluids (e.g., pumps, compressors) fitted with advanced leak-preventive seal technologies (e.g., stuffing box, double mechanical seal, canned pump with magnetic drive)? *Scale:* *1. Minimal adoption (≤ 25 %): Most equipment still uses conventional single packing or single seals.* *2. Basic adoption (25 – 49 %): Some hazardous-service equipment has been upgraded to advanced leak-preventive seal technologies.* *3. Moderate adoption (50 – 74 %): Over half of the targeted equipment has been upgraded to advanced leak-preventive seal technologies.* *4. High adoption (75 - 89 %): The great majority of the equipment uses double seal-less technology.* *5. Very high adoption (≥ 90 %): Virtually every relevant equipment is protected by dual seals or seal-less designs, aligning with industry standards (e.g., API 682 / 685) expectations for hazardous services.*
PI-13	TF	A2	P	Percentage of equipment with secondary-containment systems installed and operational to mitigate the impact of leaks. *Scale:* *1. Very Low Coverage: < 25 % of relevant equipment has an operational secondary containment system.* *2. Low Coverage: 25 – 49 % of relevant equipment has an operational secondary containment system.* *3. Moderate Coverage: 50 – 74 % of relevant equipment has an operational secondary containment system.* *4. High Coverage: 75 – 89 % of relevant equipment has an operational secondary containment system.* *5. Very High Coverage: ≥ 90 % of relevant equipment has an operational secondary containment system.*

Code	Dis.	Cap.	Type	Indicator
PI-14	TF	A2	P	Percentage of critical equipment covered by an automated early-detection system for toxic, fire, or explosion incidents. *Scale:* *1. Very low coverage: < 25 % of critical equipment is protected by an automated early-detection system.* *2. Low coverage: 25 – 49 % of critical equipment is protected by an automated early-detection system.* *3. Moderate coverage: 50 – 74 % of critical equipment is protected by an automated early-detection system.* *4. High coverage: 75 – 89 % of critical equipment is protected by an automated early-detection system.* *5. Very high coverage: ≥ 90 % of critical equipment is protected by an automated early-detection system.*
PI-15	TF	A2	P	Percentage of major-accident hazards (MAH) with at least two independent, operational safety measures in place. *Scale:* *1. Very low coverage: < 25 % of MAHs have two independent, operational safety measures.* *2. Low coverage: 25 – 49 % of MAHs have two independent, operational safety measures.* *3. Moderate coverage: 50 – 74 % of MAHs have two independent, operational safety measures.* *4. High coverage: 75 – 89 % of MAHs have two independent, operational safety measures.* *5. Very high coverage: ≥ 90 % of MAHs have two independent, operational safety measures.*
PI-16	TF	A2	P	Percentage of detected cyber/physical-security breaches that are automatically mitigated by system defence protocols. *Scale:* *1. Very low coverage: < 25 % of detected breaches are mitigated automatically.* *2. Low coverage: 25 – 49 % of detected breaches are mitigated automatically.* *3. Moderate coverage: 50 – 74 % of detected breaches are mitigated automatically.* *4. High coverage: 75 – 89 % of detected breaches are mitigated automatically.* *5. Very high coverage: ≥ 90 % of detected breaches are mitigated automatically.*

Code	Dis.	Cap.	Type	Indicator
PI-17	TF	A3	P	After each leak event of an equipment, to what extent does the site implement a containment upgrade (e.g., double-wall piping, improved diking, new leak trays) within 12 months? *Scale:* *1. Very low adaptation: Most of the leak events end with "repair in kind"; upgrades are rare (< 25 %).* *2. Low adaptation: 25 – 49 % of leak events lead to a design or containment upgrade within a year.* *3. Moderate adaptation: 50 – 74 % of leak events prompt a permanent upgrade within a year.* *4. High adaptation: 75 – 89 % of leak events prompt a permanent upgrade within a year.* *5. Very high adaptation: ≥ 90 % leaks trigger a permanent containment upgrade within a year.*
PI-18	TF	A4	P	For the past two years, to what extent the joint safety-and-security drills for technical-failure scenarios have met all predefined effectiveness criteria in the post-drill evaluation. *Scale:* *1. Very low effectiveness: < 25 % of drills meet all effectiveness criteria.* *2. Low effectiveness: 25 – 49 % of drills meet all criteria.* *3. Moderate effectiveness: 50 – 74 % of drills meet all criteria.* *4. High effectiveness: 75 – 89 % of drills meet all criteria.* *5. Very high effectiveness: ≥ 90 % of drills meet all criteria.*
PI-19	TF	A4	R	Year-on-year change in the plant's insurance premium for fire, explosion, or toxic-release coverage. *Scale:* *1. Sharp increase (> +15%): Insurers perceive higher risk; repetitive incidents or weak recovery/learning.* *2. Moderate increase (+6 % to +15 %): Some risk factors still unresolved; improvement measures not yet reflected.* *3. Stable (–5 % to +5 %): Premium roughly flat; recovery and learning meet industry norms.* *4. Moderate decrease (–6 % to –15 %): Insurers recognise better loss prevention and post-incident improvement.* *5. Sharp decrease (< –15 %): Very positive indicator of robust recovery, learning, and continuous improvement—risk profile markedly improved.*

Code	Dis.	Cap.	Type	Indicator
PI-20	MF	A1	M	Over the last three years, how many top-management–initiated safety / security actions (e.g., new policy, budget line, or "walk-the-talk" directive) have led to a tangible improvement in operating procedures or safety/security measures? *Scale:* *1. Very low commitment (0-1 improvement): Senior management seldom drives policy changes that translate into real safety or security upgrades.* *2. Low Commitment (2-3 improvements): Occasional policy initiatives reach the shop floor, but momentum is limited.* *3. Moderate improvement (4-6 improvements): A steady flow of management-led actions results in visible improvements.* *4. High commitment (7-10 improvements): Management frequently turns policy into concrete upgrades and enhanced procedures.* *5. Very high commitment (>10 improvements): Leadership demonstrates a continuous "walk-the-talk" approach; many initiatives have yielded operating or hardware gains.*
PI-21	MF	A1	P	Proportion of major hazards installations whose formal safety risk analysis (e.g., HAZOP, PHA, FTA) has been completed or re-validated within the prescribed review cycle. *Scale:* *1. Very low coverage: < 25 % of installations have an up-to-date safety risk analysis.* *2. Low coverage: 25 – 49 % of installations have an up-to-date safety risk analysis.* *3. Moderate coverage: 50 – 74 % of installations have an up-to-date safety risk analysis.* *4. High coverage: 75 – 89 % of installations have an up-to-date safety risk analysis.* *5. Very high coverage: ≥ 90 % of installations have an up-to-date safety risk analysis.*

Code	Dis.	Cap.	Type	Indicator
PI-22	MF	A1	P	Percentage of facility areas/installations whose formal security-risk analysis (e.g., Security Vulnerability Assessment [SVA], attack-tree study) has been completed or re-validated within the required review cycle. *Scale:* *1. Very low coverage: < 25 % of relevant areas/ installations have an up-to-date security risk analysis.* *2. Low coverage: 25 – 49 % of relevant areas/ installations have an up-to-date security risk analysis.* *3. Moderate coverage: 50 – 74 % of relevant areas/ installations have an up-to-date security risk analysis.* *4. High coverage: 75 – 89 % of relevant areas/ installations have an up-to-date security risk analysis.* *5. Very high coverage: ≥ 90 % of relevant areas/ installations have an up-to-date security risk analysis.*
PI-23	MF	A2	P	During incidents or emergency drills, to what extent are emergency response decisions (e.g., alarm activation, unit shutdown, public notification) executed within their predefined timeframe and success criteria? *Scale:* *1. Very low effectiveness: Most decisions or actions are late or unsuccessful.* *2. Low effectiveness: Fewer than half of the decisions or actions meet time and success criteria.* *3. Moderate effectiveness: More than half of the decisions or actions meet time and success criteria.* *4. High effectiveness: More than three-quarters of the decisions or actions meet time and success criteria.* *5. Very high effectiveness: Nearly all the decisions or actions meet time and success criteria.*
PI-24	MF	A3	P	After an incident investigation report that calls for changes to emergency-response protocols, how quickly are the affected protocols usually reviewed and updated? *Scale:* *1. Very slow: Less than half of the related protocols are updated within a year after the investigation.* *2. Slow: Over half of the related protocols are updated within a year after the investigation.* *3. Moderate: All the related protocols are updated within a year after the investigation.* *4. Fast: All the related protocols are reviewed and updated within 1–6 months after the investigation.* *5. Very fast: All the related protocols are reviewed and updated within a month after the investigation.*

Code	Dis.	Cap.	Type	Indicator
PI-25	MF	A3	P	Percentage of recommendations from formal safety risk analyses (e.g., HAZOP, LOPA, FTA) that are implemented within the target due date specified in the study action list. *Scale:* *1. Very low adaptation: < 25 % of study recommendations are implemented on or before the due date.* *2. Low adaptation: 25 – 49 % of study recommendations are implemented on or before the due date.* *3. Moderate adaptation: 50 – 74 % of study recommendations are implemented on or before the due date.* *4. High adaptation: 75 – 89 % of study recommendations are implemented on or before the due date.* *5. Very high adaptation: ≥ 90 % of study recommendations are implemented on or before the due date.*
PI-26	MF	A3	P	Percentage of recommendations from security risk analyses (e.g., SVA, Attack tree study) that are implemented within the target due date specified in the study action list. *Scale:* *1. Very low adaptation: < 25 % of study recommendations are implemented on or before the due date.* *2. Low adaptation: 25 – 49 % of study recommendations are implemented on or before the due date.* *3. Moderate adaptation: 50 – 74 % of study recommendations are implemented on or before the due date.* *4. High adaptation: 75 – 89 % of study recommendations are implemented on or before the due date.* *5. Very high adaptation: ≥ 90 % of study recommendations are implemented on or before the due date.*

Code	Dis.	Cap.	Type	Indicator
PI-27	MF	A4	R	Estimated annual financial impact of all disruptions (direct repair + downtime + lost productivity, etc.) expressed as an order-of-magnitude relative to annual site revenue. *Scale:* *1. Very high impact: Disruptions cause a loss of more than 4% of the annual revenue.* *2. High impact: Disruptions cause a loss of between 3 to 4% of the annual revenue.* *3. Moderate impact: Disruptions cause a loss of between 2 to 3% of the annual revenue.* *4. Low impact: Disruptions cause a loss of between 1 to 2% of the annual revenue.* *5. Very low impact: Disruptions cause a loss of less than 1% of the annual revenue.*
PI-28	MF	A4	M	The percentage of managers and senior managers who have completed at least one formal crisis management training in the last two years. *Scale:* *1. Very low coverage: < 25 % of senior managers completed the crisis management training.* *2. Low coverage: 25 – 49 % of senior managers completed the crisis management training.* *3. Moderate coverage: 50–74 % of senior managers completed the crisis management training.* *4. High coverage: 75 – 89 % of senior managers completed the crisis management training.* *5. Very high coverage: ≥ 90 % of senior managers completed the crisis management training.*
PI-29	LD	A1	P	Percentage of scheduled labour-relations meetings in the past year that met all three criteria: (a) held on schedule (quarterly), (b) attendance ≥ 80 % of invited participants, and (c) participant satisfaction ≥ 80 %. *Scale:* *1. Very low coverage: < 25 % of the meetings met all three criteria.* *2. Low coverage: 25 – 49 % of the meetings met all three criteria.* *3. Moderate coverage: 50 – 74 % of the meetings met all three criteria.* *4. High coverage: 75 – 89 % of the meetings met all three criteria.* *5. Very high coverage: ≥ 90 % of the meetings met all three criteria.*

Code	Dis.	Cap.	Type	Indicator
PI-30	LD	A2	P	The percentage of critical processes that can continue operating safely and securely without on-site human intervention during a labour disruption. *Scale:* *1. Very low independence: < 25 % of critical processes can run unmanned; most must stop or need major emergency measures.* *2. Low independence: 25 – 49 % of critical processes can run unmanned; the remainder require significant manual support or workarounds.* *3. Moderate independence: 50 – 74 % of critical processes can run unmanned, with on-site oversight needed for the rest.* *4. High independence: 75 – 89 % of critical processes can run unmanned, with only minor human roles or remote checks.* *5. Very high independence: ≥ 90 % of critical processes can run fully unmanned; no human measures are needed.*
PI-31	LD	A3	P	Percentage of recommendations from staffing level assessments that were executed within the agreed timelines. *Scale:* *1. Very low coverage: < 25 % of recommendations were executed on time.* *2. Low coverage: 25 – 49 % of recommendations were executed on time.* *3. Moderate coverage: 50 – 74 % of recommendations were executed on time.* *4. High coverage: 75 – 89 % of recommendations were executed on time.* *5. Very high coverage: ≥ 90 % of recommendations were executed on time.*
PI-32	LD	A4	R	Percentage of employees who “agree” or “strongly agree” in the annual satisfaction survey that workplace conditions are safe, secure, and conducive. *Scale:* *1. Very low coverage: < 25 % of employees agree or strongly agree on the statement.* *2. Low coverage: 25 – 49 % of employees agree or strongly agree on the statement.* *3. Moderate coverage: 50 – 74 % of employees agree or strongly agree on the statement.* *4. High coverage: 75 – 89 % of employees agree or strongly agree on the statement.* *5. Very high coverage: ≥ 90 % of employees agree or strongly agree on the statement.*

Code	Dis.	Cap.	Type	Indicator
PI-33	ND	A1	P	Percentage of critical infrastructure assets covered by up-to-date natural hazard risk assessments and mitigation plans (e.g., flood, seismic, blackout) completed or refreshed within the last three years. *Scale:* *1. Very low coverage: < 25 % of critical assets have up-to-date assessments and plans.* *2. Low coverage: 25 – 49 % of critical assets have up-to-date assessments and plans.* *3. Moderate coverage: 50 – 74 % of critical assets have up-to-date assessments and plans.* *4. High coverage: 75 – 89 % of critical assets have up-to-date assessments and plans.* *5. Very high coverage: ≥ 90 % of critical assets have up-to-date assessments and plans.*
PI-34	ND	A2	P	Percentage of critical equipment with tested backup power capability to sustain operation during a regional blackout. *Scale:* *1. Very low coverage: < 25 % of critical equipment have tested backup power.* *2. Low coverage: 25 – 49 % of critical equipment have tested backup power.* *3. Moderate coverage: 50 – 74 % of critical equipment have tested backup power.* *4. High coverage: 75 – 89 % of critical equipment have tested backup power.* *5. Very high coverage: ≥ 90 % of critical equipment have tested backup power.*
PI-35	ND	A3	P	Percentage of mitigation actions recommended in the latest natural hazard risk assessment (or past-event review) that are incorporated into infrastructure or process plans within 12 months of the report. *Scale:* *1. Very low adaptation: < 25 % of recommended mitigation actions are integrated within 12 months.* *2. Low adaptation: 25 – 49 % of recommended mitigation actions are integrated within 12 months.* *3. Moderate adaptation: 50 – 74 % of recommended mitigation actions are integrated within 12 months.* *4. High adaptation: 75 – 89 % of recommended mitigation actions are integrated within 12 months.* *5. Very high adaptation: ≥ 90 % of recommended mitigation actions are integrated within 12 months.*

Code	Dis.	Cap.	Type	Indicator
PI-36	ND	A4	P	In the last three years, to what extent have lessons from your most recent natural hazard drill been integrated across the following areas: a) Procedure updates; b) Training and drills; c) Infrastructure improvements; d) Technology adoption; e) Stakeholder coordination. *Scale:* *1. Very low integration: Lessons were integrated into 0–1 of the predefined areas.* *2. Low integration: Lessons were integrated into 2 of the predefined areas.* *3. Moderate integration: Lessons were integrated into 3 of the predefined areas.* *4. High integration: Lessons were integrated into 4 of the predefined areas.* *5. Very high integration: Lessons were integrated into 5 of the predefined areas.*
PI-37	TS	A1	P	Percentage of critical infrastructure assets protected by at least three independent physical/cyber-security layers and tested within the past 12 months. *Scale:* *1. Very low coverage: < 25 % of critical assets have ≥ 3 security layers tested in the last year.* *2. Low coverage: 25 – 49 % of critical assets have ≥ 3 security layers tested in the last year.* *3. Moderate coverage: 50 – 74 % of critical assets have ≥ 3 security layers tested in the last year.* *4. High coverage: 75 – 89 % of critical assets have ≥ 3 security layers tested in the last year.* *5. Very high coverage: ≥ 90 % of critical assets have ≥ 3 security layers tested in the last year.*
PI-38	TS	A1	P	Frequency of software updates or firmware patches applied to critical control systems (e.g., DCS, SIS controller, network firewalls) per year. *Scale:* *1. Very low frequency: On average, < 1 update per year.* *2. Low frequency: On average, 1 – 2 updates per year.* *3. Moderate frequency: On average, 3 – 5 updates per year.* *4. High frequency: On average, 6 – 11 updates per year.* *5. Very high frequency: On average, ≥ 12 updates per year.*

Code	Dis.	Cap.	Type	Indicator
PI-39	TS	A2	P	On average, how quickly were unauthorized access or security breach attempts detected and responded to by the security systems or personnel? *Scale:* *1. Very low speed, > 15 minutes: Intruder can wander freely for long periods.* *2. Low speed, 8 - 15 minutes: Noticeable delays leave windows for damage or theft.* *3. Moderate speed, 4 - 7 minutes: Response is workable but slow; gaps remain in monitoring or staffing.* *4. High speed, 1- 3 minutes: Rapid containment on most attempts; only occasional slowdowns.* *5. Very high speed, ≤ 1 minute: Intrusions are intercepted almost instantly.*
PI-40	TS	A3	P	How quickly are security protocols reviewed and updated after a vulnerability assessment or incident investigation report? *Scale:* *1. Very slow, > 12 months: Protocols rarely get updated within a year.* *2. Slow, 7 – 12 months: Updates often take over half a year to complete.* *3. Moderate, 4 – 6 months: Updates generally finish within 6 months.* *4. Fast, 1 – 3 months: Updates are usually within a quarter.* *5. Very fast, ≤ 1 month: Updates are rolled out within a few weeks.*
PI-41	TS	A4	M	Percentage of relevant personnel who complete retraining on updated security protocols within one year of the protocol change. *Scale:* *1. Very low coverage: < 25 % of personnel retrained within one year.* *2. Low coverage: 25 – 49 % of personnel retrained within one year.* *3. Moderate coverage: 50 – 74 % of personnel retrained within one year.* *4. High coverage: 75 – 89 % of personnel retrained within one year.* *5. Very high coverage: ≥ 90 % of personnel retrained within one year.*

Code	Dis.	Cap.	Type	Indicator
PI-42	TS	A4	P	Last two years, what percentage of joint safety-security drills for terrorism/sabotage scenarios met the predefined effectiveness criteria in post-drill evaluations? *Scale:* *1. Very low effectiveness: The drills met 25 % of the effectiveness criteria.* *2. Low effectiveness: The drills met 25 – 49 % of the effectiveness criteria.* *3. Moderate effectiveness: The drills met 50 – 74 % of the effectiveness criteria.* *4. High effectiveness: The drills met 75 – 89 % of the effectiveness criteria.* *5. Very high effectiveness: The drills met ≥ 90 % of the effectiveness criteria.*
PI-43	SC	A1	P	Percentage of raw material items that have two or more qualified suppliers contracted for normal or contingency supply. *Scale:* *1. Very Low Coverage: < 25 % of raw material items have two or more qualified suppliers.* *2. Low coverage: 25 – 49 % of raw material items have two or more qualified suppliers.* *3. Moderate coverage: 50 – 74 % of raw material items have two or more qualified suppliers.* *4. High coverage: 75 – 89 % of raw material items have two or more qualified suppliers.* *5. Very high coverage: ≥ 90 % of raw material items have two or more qualified suppliers.*
PI-44	SC	A2	P	Percentage of critical inventory within a sufficient buffer level to sustain operation during supply chain disruptions. *Scale:* *1. Very low coverage: < 25 % of critical inventory items are at or above their buffer stock level.* *2. Low coverage: 25 – 49 % of critical inventory items are at or above their buffer stock level.* *3. Moderate coverage: 50 – 74 % of critical inventory items are at or above their buffer stock level.* *4. High coverage: 75 – 89 % of critical inventory items are at or above their buffer stock level.* *5. Very high coverage: ≥ 90 % of critical inventory items are at or above their buffer stock level.*

Code	Dis.	Cap.	Type	Indicator
PI-45	SC	A3	P	Percentage of recommendations from annual supplier reliability and quality assessments that are implemented within the agreed timelines. *Scale:* *1. Very low adaptation: < 25 % of supplier assessment recommendations are implemented on time.* *2. Low adaptation: 25 – 49 % of supplier assessment recommendations are implemented on time.* *3. Moderate adaptation: 50 – 74 % of supplier assessment recommendations are implemented on time.* *4. High adaptation: 75 – 89 % of supplier assessment recommendations are implemented on time.* *5. Very high adaptation: ≥ 90 % of supplier assessment recommendations are implemented on time.*
PI-46	SC	A4	R	Reduction in the number of supply chain-related operational disruptions year-on-year. *Scale:* *1. Very low improvement: Disruptions have increased, or the reduction is less than 0 %.* *2. Low improvement: Disruptions reduced by 0 – 4 % compared to last year.* *3. Moderate improvement: Disruptions reduced by 5 – 9 % compared to last year.* *4. High improvement: Disruptions reduced by 10 – 14 % compared to last year.* *5. Very high improvement: Disruptions reduced by 15 % or more compared to last year.*
PI-47	SH	A1	P	Percentage of external stakeholders who satisfy ≥ 80 % of the predefined engagement criteria during annual assessment. *Scale:* *1. Very low coverage: < 25 % of stakeholders meet ≥ 80 % of the engagement criteria.* *2. Low coverage: 25 – 49 % of stakeholders meet ≥ 80 % of the engagement criteria.* *3. Moderate coverage: 50 – 74 % of stakeholders meet ≥ 80 % of the engagement criteria.* *4. High coverage: 75 – 89 % of stakeholders meet ≥ 80 % of the engagement criteria.* *5. Very high coverage: ≥ 90 % of stakeholders meet ≥ 80 % of the engagement criteria.*

Code	Dis.	Cap.	Type	Indicator
PI-48	SH	A2	P	How resilient is the operation in continuing safely and securely under external social hazards (e.g., protests, pandemics, utility provider strikes)? *Scale:* *1. Very low resilience: Operation halts or is severely compromised if external social hazards occur. The facility lacks fallback procedures or resources to address workforce shortages or utility interruptions.* *2. Low resilience: Operation can run at limited capacity during external social hazards but relies on major or ad hoc measures. Some fallback resources exist, but workforce or utility constraints remain a significant risk.* *3. Moderate resilience: Operation can continue in a reduced mode with some established contingency plans. Partial redundancy and workforce flexibility are in place, but disruptions are still noticeable.* *4. High resilience: Operation runs near normal under moderate external social hazards, thanks to robust contingency plans and workforce cross-training. Impacts on production and workforce safety are limited.* *5. Very high resilience: Operation is largely unaffected by external social hazards, relying on well-developed contingency procedures, alternative supply lines, and strong workforce adaptability. Minimal to no direct impact on production or worker security.*
PI-49	SH	A3	P	Percentage of recommendations from external stakeholders' reviews/ engagement program that are completed within the agreed timelines for the last two years. *Scale:* *1. Very low adaptation: < 25 % of recommendations are completed on time.* *2. Low adaptation: 25 – 49 % of recommendations are completed on time.* *3. Moderate adaptation: 50 – 74 % of recommendations are completed on time.* *4. High adaptation: 75 – 89 % of recommendations are completed on time.* *5. Very high adaptation: ≥ 90 % of recommendations are completed on time.*

Code	Dis.	Cap.	Type	Indicator
PI-50	SH	A4	P	Percentage of business continuity plan and response procedures for external social hazards that have been reviewed and improved within the last three years. *Scale:* *1. Very low improvement: < 25 % of relevant procedures have been reviewed and improved in 3 years.* *2. Low improvement: 25 – 49 % of relevant procedures have been reviewed and improved in 3 years.* *3. Moderate improvement: 50 – 74 % of relevant procedures have been reviewed and improved in 3 years.* *4. High improvement: 75 – 89 % of relevant procedures have been reviewed and improved in 3 years.* *5. Very high improvement: ≥ 90 % of relevant procedures have been reviewed and improved in 3 years.*

Appendix D

Context mapping headings and example observations used to support interpretation for Plant M and Plant N

Context mapping heading	Plant M example observations	Plant N example observations	How it was used in interpretation
1. Organisational setting and governance	Single-operator plant setting with plant-centred decision-making for most operational controls within the assessed boundary	Multi-operator industrial complex setting; some cross-cutting arrangements coordinated at complex level, with site-user responsibilities bounded accordingly	Supported interpretation of cross-case differences in baseline patterns and clarified when differences reflected governance structure rather than "performance"
2. Roles, ownership, and coordination mechanisms (safety and security)	Cross-functional roles available within the plant to discuss and evidence safety and security practices during workshop operationalization	Safety and security responsibilities distributed across organisational layers; some arrangements owned externally, requiring reliance on key-informant visibility	Informed boundary setting and "N/A" decisions; explained ownership-driven interpretability limits, especially for security-related indicators
3. Major-hazard governance context and evidence infrastructure	Major-hazard obligations shaped documentation and routine evidence sources (management system records, audits, emergency preparedness artifacts) used during scoring	Seveso-type obligations shaped site-user evidence sources within an industrial-complex governance environment	Helped explain why certain safety-related evidence was available and comparable across cases, and why some security evidence was less directly observable at plant level

Context mapping heading	Plant M example observations	Plant N example observations	How it was used in interpretation
4. Operational scope and complexity factors	Focal operational areas used to anchor discussions and evidence gathering; operational routines observed during engagement	Emphasis on site-level arrangements plus process and logistics interfaces; external interactions shaped exposure and evidencability	Supported interpretation of disruption domains where interfaces matter (e.g., labour disruption continuity, external social hazards, logistics), and where evidence expectations differ
5. Access pathway and implementation feasibility conditions	Embedded engagement plus cross-functional workshop enabled consistent anchor interpretation and efficient disruption-by-disruption progression	Bounded access required iterative engagement primarily through a key informant, supported by follow-up clarification and available documents	Explained differences in N/A coverage and confidence for certain indicators, and framed implementation enablers/constraints without treating bounded access as a methodological deficiency

Note: The context map was maintained as structured notes (and where available, supporting documents) and used to (i) clarify assessment boundaries and "N/A" decisions, (ii) interpret baseline patterns and cross-case contrasts, and (iii) explain implementation enablers and constraints rather than evaluate regulatory performance.

Appendix E

Operationalization artifacts and outputs produced in case studies during RoPSS application

Output / artifact	Plant M	Plant N
System boundary and focal areas	Overall plant system, HCl synthesis unit, and methyl chloride storage area	Site-level arrangements, core manufacturing process, and logistics/ loading interfaces (bounded by access conditions)
Context map (governance, roles, complexity, regulatory context)	Compiled from on-site engagement and cross-functional input	Compiled from documents and key-informant explanations
Disruption structuring record (eight disruption categories)	Used as prompts in workshop discussions	Used as prompts in structured discussions and questionnaires
Instrument package used	Same RoPSS indicator set and structured questionnaires, completed in a workshop (6–7 May 2025)	Same RoPSS indicator set and structured questionnaires, completed May–June 2025 through iterative, documented discussions
Anchor interpretation and clarification notes	Clarifications recorded during facilitated sessions alongside scoring	Clarifications recorded through iterative spreadsheet review and meetings
Completed scoring sheets with evidence rationales and N/A log	1–5 scores recorded with brief rationales; “N/A” items marked and excluded from averages	1–5 scores recorded with brief rationales; evidence availability noted; “N/A” items marked and excluded from averages
Baseline profiles (capability and heatmap outputs)	4As capability averages and disruption × capability heatmaps (A1–A4)	4As capability averages and disruption × capability heatmaps (A1–A4)
Diagnostic narrative (strengths and gaps)	Key strengths and vulnerabilities derived from profiles and workshop discussions	Key strengths and vulnerabilities derived from profiles and discussions, with bounded interpretation noted

Output / artifact	Plant M	Plant N
Step 6 outputs (resilience-enhancing strategies)	Candidate actions/projects/ programmes captured during the workshop	Candidate actions and improvement suggestions captured through discussions and questionnaire inputs
Usability reflections (clarity, measurability, feasibility)	Practitioner reflections captured during sessions and workshop	Key-informant reflections captured, including feedback on measurability and the need for qualitative scoring for selected indicators
Implementation log and anonymized evidence archive	Dated engagement phases; templates, anonymized notes, and aggregated outputs retained (confidential)	Dated iterative engagement; templates, anonymized notes, and aggregated outputs retained (confidential)



Appendix F

Online research dataset

The dataset provides supporting materials underlying the survey, semi-structured interviews, expert elicitation, and case study components of the doctoral research. It is intended to enhance transparency, traceability, and reusability of the study materials and selected research outputs.

The dataset can be publicly accessed at 4TU.ResearchData through this link: https://doi.org/10.4121/54e0fb03-911a-4b24-a49b-31b88e45f4f3

The dataset includes:

1. a README file;
2. a survey questionnaire;
3. anonymized survey data;
4. an interview consent form template;
5. an interview protocol and guide;
6. an interview codebook;
7. Thematic Analysis Matrices (TAMs) with selected anonymized interview quotations;
8. an expert elicitation dataset for assessing the importance and availability of performance indicators; and
9. case study data on the operationalization of the RoPSS framework in two chemical plants.

Acknowledgements

All praise and gratitude are due to Allah Almighty, whose mercy, guidance, and blessings have carried me through this long journey.

I was born into a family where higher education was not a natural path, but a distant possibility. My parents did not have the opportunity to pursue higher education, and such opportunities were limited within my family. As the fifth of seven children, I was fortunate to continue my studies from a bachelor's degree to a master's degree and eventually a PhD. This journey has never belonged to me alone. It carries the prayers, sacrifices, and hopes of my family, the steadfast support of my wife, and our shared hope of opening a wider path for our children and the generations after us.

This thesis is therefore dedicated to my beloved family. To my late mother, whose love, prayers, and sacrifices remain with me in every step of this journey, even though she is no longer here to witness its completion; to my father, whose perseverance and quiet strength have shaped the person I am today; to my wife, Raihana, thank you for walking beside me through the difficult and beautiful moments of this PhD journey, and for your patience, sacrifices, and unwavering support; to my children, Rayyan and Raisha, you are my greatest source of joy, strength, and motivation. I hope this work will one day remind you of the value of courage, perseverance, and gratitude in pursuing a meaningful life. To my siblings, and to my father- and mother-in-law, thank you for your prayers, encouragement, and love. This achievement belongs to all of you.

My deepest gratitude goes to my supervisor and promotor, Prof. Genserik Reniers. Back in Malaysia, while preparing my scholarship research proposal, I came across one of your articles. That article sparked my interest not only in the topic, but also in the possibility of working with you as a PhD candidate. I still remember emailing you and receiving your prompt and encouraging response. Even before I began my PhD at TU Delft, you had already taken the time to provide constructive and helpful feedback on my proposal. Throughout these four years, you have guided me with kindness, clarity, and wisdom. You encouraged me when I needed confidence, offered useful suggestions when I needed direction, corrected me when I was wrong, and complimented me when I had done well. I could not have asked for a better mentor and supervisor.

I am equally grateful to my daily supervisor, Prof. Ming Yang, for his constant guidance, patience, and support throughout this PhD journey. Thank you for walking closely with me through the many stages of this research, from shaping ideas and refining arguments to improving manuscripts and responding to reviewers. Your careful feedback, critical questions, and calm encouragement helped me to think more clearly and write more confidently. I am especially grateful for the time and attention you gave to my work, and for the trust you placed in me as I developed as a researcher. Your supervision has been an essential part of this thesis and of my growth during these four years.

I am deeply grateful to all the academic mentors and teachers who shaped my journey long before this thesis came into being. My sincere appreciation goes to my teachers at Sekolah Menengah Sains Kota Tinggi (SAKTI), Johor, where I spent five formative years from the age of thirteen. Those years taught me discipline, independence, resilience, and the courage to dream beyond the circumstances into which I was born. I also extend my gratitude to my lecturers and mentors at Universiti Teknologi Malaysia, where I pursued my bachelor's degree, and at Universiti Teknologi PETRONAS, where I completed my master's degree. Each of you contributed, in your own way, to the foundation that allowed me to arrive at this stage. I am also grateful to Prof. Azmi Mohd Shariff for his guidance and support as my external adviser, and for remaining an important link to my academic roots in Malaysia.

Before this PhD, much of my understanding of safety was shaped not in lecture halls, but through my years of service at the Department of Occupational Safety and Health (DOSH) Malaysia. I am deeply grateful to my superiors, colleagues, and friends at DOSH, especially those at the Kuala Lumpur state office, where I served for ten years, and at DOSH headquarters in Putrajaya, where I served for four years. The lessons I learned there, both technical and human, became an important foundation for this research.

I gratefully acknowledge the Public Service Department of Malaysia for awarding me the scholarship that made this PhD possible. I am also deeply thankful to the top management of DOSH for their support and trust in allowing me to pursue this doctoral study. This opportunity has been both a privilege and a responsibility, and I hope that the knowledge and

experience gained through this journey will contribute in meaningful ways to the advancement of occupational safety and health, process safety, and process security in Malaysia.

I am also grateful to my friends and colleagues at TU Delft: Ashraf, Wei Jun, Shuaiqi, Yuanyuan, Rongxin, Xin Ren, Rioshar, Rustam, Giorgia, Jelle, Karolien, and many others. Many of you have already completed your own journeys and moved on to new chapters, but the conversations, lunches, coffees, laughter, and small moments we shared made my years in Delft warmer and more meaningful.

I would also like to express my sincere gratitude to the industry practitioners, government officials, expert interviewees, and survey respondents who generously contributed their time, experience, and insights to this research. Your openness in sharing practical perspectives on process safety, process security, and resilience made this thesis richer and more grounded in real-world practice. I am especially grateful to Dr. Peter Schmitz, Fairuz Anwar, Kasman Nasir, and Yunus Yusop for their support, advice, and willingness to connect me with relevant people and opportunities. This research would not have been possible without the trust, generosity, and professional wisdom of all those who contributed along the way.

Looking back, this PhD has been more than an academic pursuit. It has been a journey of leaving, learning, striving, and growing. It took my family and me far from the familiarity of home, brought us into a new country and culture, and introduced me to people whose kindness, wisdom, and generosity have shaped this chapter of my life. In many ways, it reminds me of a poem attributed to the great Islamic scholar Imam al-Shafi'i (767–820 CE), rendered in English as:

A learned and well-mannered person does not remain stationary in his homeland,
So leave your home and strive hard,
For the sweetness of life is found in striving.

I have seen that water stagnates if it remains still,
If it flows, it becomes clear and pure,
But if it stops, it becomes murky and spoils.

The arrow, if it does not leave its bow,
Will never strike its target.

The rare aloeswood is no different from ordinary wood,
If it remains ungathered, hidden away in the forest.

Leave your country in search of loftiness and travel,
For in travel there are five benefits:
relief of adversity and anxiety,
earning of a livelihood,
acquisition of knowledge,
learning of etiquettes and culture,
and companionship of the noble.

May this journey be a reminder to myself, my beloved wife, Raihana, and especially my children, Rayyan and Raisha, that where we begin does not determine how far we may go. May whatever blessings and opportunities we are given be carried with gratitude, humility, and the courage to keep growing.

Muhammad Shah Bin Ab Rahim
Voorburg, the Netherlands

Curriculum Vitae

Muhammad Shah Bin Ab Rahim was born in Kangkar Tebrau, Johor, Malaysia. He obtained his Bachelor of Engineering (Chemical) degree from Universiti Teknologi Malaysia, Skudai, Malaysia, in 2006. He later pursued a Master of Science in Process Safety at Universiti Teknologi PETRONAS, Malaysia, which he completed in 2018.

From 2007 to 2008, he worked as an R&D Engineer at Shin-Etsu Electronics (Malaysia) Sdn. Bhd., where he was involved in the development of epoxy moulding compound formulations for the semiconductor industry.

In 2008, Muhammad Shah joined the Department of Occupational Safety and Health (DOSH) Malaysia, where he served as Principal Assistant Director until 2022, before pursuing his doctoral studies. At DOSH, his work included occupational safety, process safety, and industrial hygiene workplace inspections, as well as contributions to the development of the National Occupational Safety and Health Master Plan for 2021 to 2025. During his service, he received the Excellent Service Award from the Ministry of Human Resources Malaysia in 2010 and 2020.

In September 2022, Muhammad Shah joined the Safety and Security Science research group at the Faculty of Technology, Policy and Management, Delft University of Technology, the Netherlands, as a PhD researcher. His doctoral research focused on the integration of process safety and process security risk management through a resilience-oriented framework.

During his PhD research, he was also involved in a project proposal exploring the scientific basis and practical needs for the transition from static to dynamic risk management in the Dutch process industries. He also contributed to teaching activities as a guest lecturer in the Methods for Risk Analysis and Management course and the Risk Management summer course. In addition, he served as a reviewer for process safety-related journals, including *Safety Science*, the *Journal of Loss Prevention in the Process Industries*, and the *Journal of Safety Science and Resilience*.

After completing his PhD, he continued his service as Principal Assistant Director at the DOSH Malaysia headquarters in Putrajaya, Malaysia. In this role, he aims to contribute to the development of national guidelines

for resilience-oriented process safety and security management in the chemical industry.

List of Publications

1. Ab Rahim, M. S., Reniers, G., Yang, M., & Bajpai, S. (2024). Risk assessment methods for process safety, process security and resilience in the chemical process industry: A thorough literature review. *Journal of Loss Prevention in the Process Industries*, *88*.
   https://doi.org/10.1016/j.jlp.2024.105274
2. Ab Rahim, M. S., Reniers, G., & Yang, M. (2024). Bridging Boundaries: Crafting a Resilient, Integrated Risk Management Model for Process Safety and Process Security. *Chemical Engineering Transactions* , *111*, 133–138.
   https://doi.org/10.3303/CET24111023
3. 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
4. Ab Rahim, M. S., Reniers, G., & Yang, M. (2025). Developing Resilience-Oriented Indicators for Integrated Process Safety and Process Security Risk Management. *Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference*.
   https://doi.org/10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P3750-cd
5. Ab Rahim, M. S., Reniers, G., & Yang, M. (2026). A resilience-oriented framework for managing process safety and process security. Process Safety and Environmental Protection, 215, 109182.
   https://doi.org/10.1016/j.psep.2026.109182
6. *Ab Rahim, M. S., Reniers, G., Yang, M., Schmitz, P., & Mhd Yusop, M. Y. (2026). Operationalizing the RoPSS framework in chemical plants: Diagnostic profiles and methodological lessons from two case studies. Safety Science (Under Review).*

