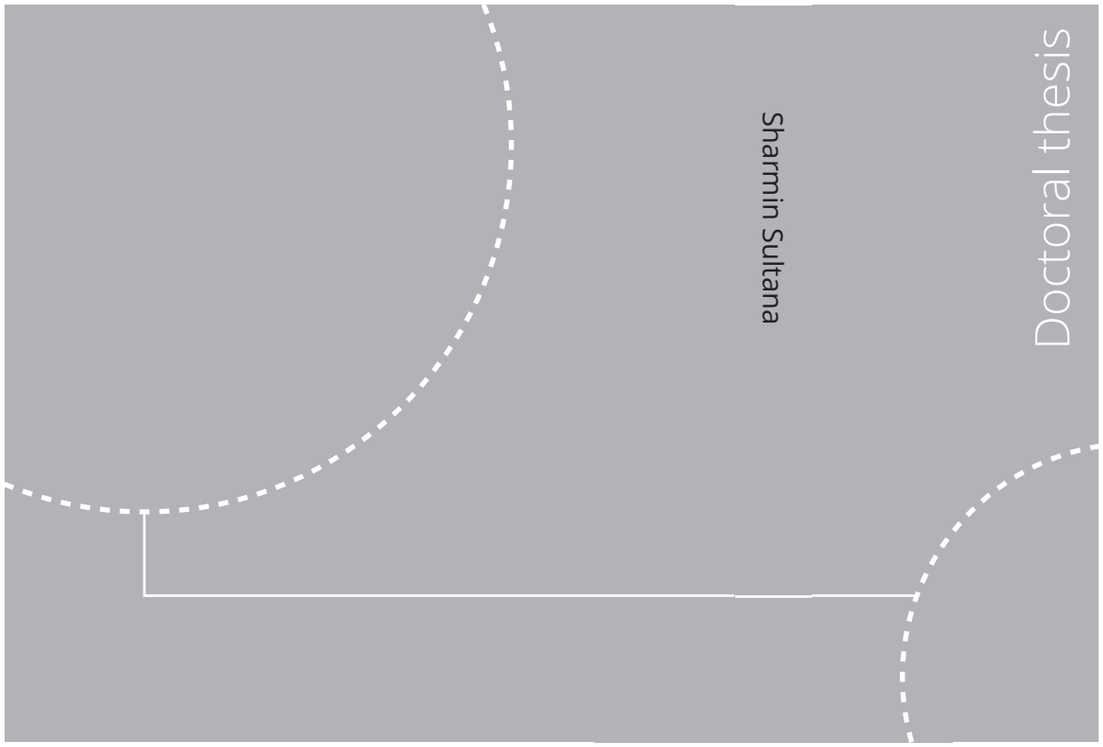
ISBN 978-82-326-5953-1 (printed ver.)
ISBN 978-82-326-6398-9 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (electronic ver.)



Doctoral theses at NTNU, 2022:323

Sharmin Sultana

Process safety and risk management using system perspectives

A contribution to the chemical process and petroleum industry

NTNU
Norwegian University of
Science and Technology
Thesis for the degree of
Philosophiae Doctor
Faculty of Engineering
Department of Marine Technology

NTNU
Norwegian University of
Science and Technology

Doctoral theses at NTNU, 2022:323

NTNU

NTNU
Norwegian University of
Science and Technology

Sharmin Sultana

Process safety and risk management using system perspectives

A contribution to the chemical process and petroleum industry

Thesis for the degree of Philosophiae Doctor

Trondheim, Nov 2022

Norwegian University of Science and Technology
Faculty of Engineering
Department of Marine Technology

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Engineering
Department of Marine Technology

ISBN 978-82-326-5953-1 (printed ver.)
ISBN 978-82-326-6398-9 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (electronic ver.)

Doctoral theses at NTNU, 2022:323

PRINTED IN NORWAY
NO - 1598

NORDIC SWAN ECOLABEL
Printed matter
2041 0731

Printed by Skipnes Kommunikasjon AS

PREFACE

This thesis is being submitted to fulfill the degree requirements, Doctor of Philosophy (Ph.D.), in the Faculty of Engineering at the Department of Marine Technology at the Norwegian University of Science and Technology (NTNU), Norway. The research has been conducted as part of a collaboration project between NTNU and DynSoL AS from 2018 to 2021. The courses have been attended as part of the degree requirement of NTNU. The Norwegian Research Council and DynSoL AS Norway have funded the project under grant number 283861.

The project has been conducted at the Department of Marine Technology at NTNU. Professor Stein Haugen has been the main Ph.D. supervisor, and Professor Jan Erik Vinnem has been the project's co-supervisor. The project has been simultaneously followed by the Department of Research and Innovation, DynSoL AS, Norway, where Kamrul Islam has been engaged as Project Manager.

The project's primary goal is to provide new knowledge concerning risk management applicable in the process and oil-gas industry. The multidisciplinary nature of the field has always delighted me. As I participated in petroleum projects as a consultant, I felt frustrated that some elements of the method and practices I observed could be improved, so I wanted to explore more.

My motivation for conducting the research is rooted in my professional background as a technical safety engineer. A career in the oil gas industry has given me insights into the practical challenges of applying methods and theoretical limitations. Hence, the topic of this thesis encompasses many distinct aspects and questions related to process safety and risk management.

Trondheim, November 2022

SUMMARY

Risk management is all activities used to manage the risk of hazardous events and provides information to improve decision-making. A typical approach to system safety is to identify and eliminate the causes of an accident after it occurs and to repeat such efforts if a new accident occurs. (Ham, 2021). A traditional approach is principally reactive (Dallat et al., 2018). With the advancement of industrial systems, e.g., integrated control and safety systems, complex operation and shutdown sequences have evolved challenges in managing risk and safety. Considering the changing nature of today's design and recent accidents, it has become vital to improve existing approaches to capture the complexity and dynamic nature of the automated system.

The overall goal of the research presented in this thesis is to improve existing methods and develop new strategies using system engineering concepts and methodology for better risk management. Safety management focuses on two stages: pre-operational and operational stages. Design improvement of the system is focused on the first stage. The related tools can be utilized in the conceptual, preliminary, and detailed design stages. At the start of the design stage, detailed hazard identification should be conducted. The tools proposed for design improvement are inherent system safety and functional safety assessment. Safety assurance in the operational phase is achieved by monitoring safety performances. For monitoring safety, a performance indicator system-based perspective is advised. Based on the monitoring, safety training, education, regulatory compliance, inspection, or maintenance can be advanced, and plans can be set accordingly.

The thesis is divided into two sections. Part I provides an overview of the risk management aspects to be considered. Part I also summarizes the main contributions of the research project. Some ideas for further work are also discussed in this part. Part II comprises six papers addressing different topics within the objective and scope of the thesis. The research focuses on various phases of the industry's challenges in risk management. The thesis considers two hazard identification techniques: STPA and HAZOP, as hazard identification as the core of risk assessment in oil and gas activities. It questions whether present existing methods can identify hazards of the modern complex systems. It also proposes necessary improvements considering the complexity and interaction of today’s design.

Present thesis discuss the topic of inherent safety and evaluation. Issues with the usage of inherent safety in the industry and practical challenges in adopting

inherent safety indices by the industry and industry personnel are discussed. The pieces of literature discussed are relevant to the process and petroleum industry. It presents various inherent hazard risk factors with practical examples pertinent to the process industry. Identifying inherent hazards and risk factors makes it easier for the user to quickly find an inherently safer solution.

The present research presents an inherent safety evaluation method for the system. The procedure is applied for a process system that validates the method's applicability. The approach finds a scientific basis for previously established parameter-based inherent safety evaluation methods. The foremost step of the technique, which is finding inherent safety characteristics and their related parameter, makes the method flexible and general to be applicable in all industry sectors. The feature of a perfect, inherently safer system and their corresponding numerical values are determined to find a logical scoring system. The deviation of a real system for those parameters is determined to determine the score of inherent safety subindices; thereby overall inherent system safety index is determined. The method removes the problems of existing approaches, like dimensionality problems, lacking the logical basis of parameter scoring.

The thesis also proposes a system engineering approach to check the adequacy of the facility's safety barriers and safety assessment. Research adopts the FRAM (Functional Resonance Analysis Method) method to find the required safety barriers in the system. A two-level mathematical model is developed to predict the system's safety. The developed method is applied with a practical case study of the Liquified Natural Gas (LNG) ship-to-ship transfer system. Furthermore, the thesis works on the development of safety performance indicators. It uses a system engineering method, System Theoretic Process Accident Model (STAMP), to develop indicators. Indicators were also developed using previously established methods like OECD (Environment, Health, and Safety Program) and CCPS (Center for chemical process safety). All the methods were applied for a case study of the LNG Floating Storage and Regasification Unit; Based on the evaluation, a comparative analysis was performed.

The contributions of the research apply to several sectors and industry branches. Through the application of the methods, it has been possible to validate the developed methods and concepts. The thesis contributes to better decision support and improved risk management. The developed and analyzed methods focus on non-probabilistic methods. It emphasizes a non-probabilistic framework that does not depend on historical data. Assigning probabilistic information to an automated system is challenging and error-prone with excessive assumptions.

However, the thesis points out the need to conduct more real case studies. Future publications should focus on applying the developed methods more straightforwardly to encourage users to use them. In addition, improved risk management methods should consider dynamic control of the automated system, which should also be focused on in future works.

ACKNOWLEDGMENTS

I offer my gratitude to the Norwegian Research Council and DynSoL AS, Norway, for providing me with the opportunity of research, assistance, and financial support to conduct the project.

I am indebted to my supervisor Professor Stein Haugen, Department of Marine Technology, NTNU. His excellent support, assistance, and patience throughout the project have helped me stay on track during the research. Without his extreme patience and guidance, the success of this project would have never been possible.

I am grateful to my co-supervisor and co-author, Professor Jan Erik Vinnem, Department of Marine Technology, NTNU, for his contributions, critiques, suggestions, and guidance while writing Paper I, Paper II, and Paper VI. I benefited from his deep insights and broad experiences.

Thanks to the management team, DynSoL AS, for encouraging me to initiate and conduct the project and keeping me updated with industrial challenges. Special thanks to Project Manager Dr. Kamrul Islam, DynSoL AS, for discussing ideas and follow-up on the project's progression. Also, thanks to Gisle Obrestad, DynSoL AS, for his administrative support during the project. I would also like to thank the other people involved at various project stages.

I am thankful to my co-authors, Dr. Jan Dahlsveen and Dr. Peter Okoh, for their contributions to Paper II and Paper I. I am grateful to co-author Professor Bjørn Sørskot Andersen, Department of Mechanical and Industrial Engineering, NTNU, for his contribution to Paper VI and for providing in-depth knowledge in the field of performance measurement. I am grateful to Professor Antonio Rauzy, Department of Mechanical and Industrial Engineering, NTNU, for providing in-depth knowledge in system engineering.

I am grateful to Professor Ingrid Bower Utne at the department of Marine Technology NTNU and Professor Bjørn Axel Gran at the Mechanical and Industrial Engineering department at NTNU for giving valuable insight into the field of system safety engineering and risk management. I would like to thank other Ph.D. students and researchers at the Department of Marine Technology for productive discussions, comments on my research, and spending time with me apart from working time. Finally, I would like to thank my parents, siblings, children, and friends for their encouragement and moral support during the work of this thesis.

CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

ABBREVIATIONS

CHAZOP	Control Hazard and Operability Study
ETA	Event Tree Analysis
FMECA	Failure mode, effect, and criticality analysis
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
HRO	High-Reliability Organization
IEC	International Electrotechnical Commission
ISI	Inherent Safety Index
ISSI	Inherent System Safety Index
I2SI	Integrated Inherent Safety
LNG	Liquified Natural Gas
OFISI	Optimizable Fuzzy Inherent Safety Index
PISI	Prototype Inherent Safety Index
QRA	Quantitative Risk Analysis
SE	System Engineering
SHE	Safety, Health, and Environment
SPI	Safety Performance Indicator
STAMP	Systems Theoretic Accident Model and Process
STPA	Systems Theoretic Process Analysis
TRIZ	Theory of Inventive Problem Solving

OVERVIEW OF APPENDED PAPERS AND CONTRIBUTION OF AUTHORS

The papers that make up the thesis, along with the author's contributions, are listed below:

Paper I. Journal paper

Sultana, S., Vinnem J.E., Okoh P., & Vinnem, J. E., (2019). Hazard analysis: Application of STPA to the ship-to-ship transfer of LNG Journal of Loss Prevention in the Process Industries, 60, 241-252 (Sultana et al., 2019b).

Contribution of authors:

The first author initiated the research idea and identified the state-of-the-art and research gaps based on which the research approach is defined. Co-authors contributed to designing and running the case study and provided support and feedback. The first author wrote the manuscript, and the co-authors supervised the whole work.

Paper II. Conference paper

Sharmin Sultana, Vinnem Jan Erik, Jan Dahlsveen, Stein Haugen. Inherent safety assessment: current state of the art and why it is still not effectively adopted by industry. The 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. 2020. Italy: Research Publishing, Singapore (Sultana et al., 2020).

Contribution of authors

The first author initiated the research idea and identified the state of the art and the research gap. Co-authors supported with expert feedback. The first author wrote the manuscript while co-authors supervised the work and provided feedback.

Paper III. Conference paper

Sultana, S., Haugen, S.., Achieving inherent safety from hazard and risk factors. In 31st European Safety and Reliability Conference ESREL 2021. Trondheim, Norway (Sultana and Haugen, 2021).

Contribution of authors

The first author initiated the research idea identifying the state of the art and existing gaps. Based on the finding, the research approach is proposed. The first author wrote the manuscript. The second author, supported with risk management expertise, supervised the work, and provided valuable feedback.

Paper IV. Journal paper

Sultana, Sharmin, and Stein Haugen. "Development of an inherent system safety index (ISSI) for ranking of chemical processes at the concept development stage." Journal of Hazardous Materials 421 (2022): 126590 (Sultana and Haugen, 2022)

Contribution of authors

The first and second authors initiated the research idea. The first author identified the state-of-the-art and research gaps based on which the research approach was defined. The first author developed the inherent safety subindices from which the overall inherent system safety index is developed, checked the application of the generated index with a case study, wrote the manuscript, and the second author supervised the work and provided valuable feedback.

Paper V. Journal paper

Sultana, Sharmin, and Stein Haugen. "An extended FRAM method to check the adequacy of safety barriers and to assess the safety of a socio-technical system." Safety Science, 157.

Contribution of authors

The first author initiated the research idea and identified the state-of-the-art and research gaps based on the adopted research approach. The first author wrote the manuscript. The second author supervised the work and provided valuable feedback.

Paper VI. Journal paper

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 (Sultana et al., 2019a).

Contribution of authors

The first author initiated the research idea. Based on the identified state-of-the-art and research gaps and research approaches were defined. The second author supported performance measurement expertise. The first author wrote the manuscript, and co-authors supervised the work and provided valuable feedback.

The below paper is not included in the main discussion. However, considering the scope, the article is included in part II.

Paper VII. Conference paper

Sultana, S., Bucelli, M., Zhang, J., Rauzy, A., How system engineering may help prepare FMECA lesson learned from a practical case. in 28th European Safety and Reliability Conference ESREL 2018. Trondheim, Norway (Sultana et al., 2018).

Contribution of authors

First, second, and third authors-initiated research ideas and identified state-of-the-art and research gaps based on the adopted research approach. The first, second, and third authors wrote the manuscript, and the fourth author supervised the work and provided valuable feedback.

Part I- Main report

1 INTRODUCTION

1.1 BACKGROUND AND MOTIVATION

As a scientific topic, risk management concepts were established in the era of 1970 and 1980s to conceptualize, assess, and manage risk (Aven, 2016). The risk field advanced in two main directions. The first is to study and treat the risk of specific activities (FDIS, 2009). Secondly, to conduct generic risk research and development involving concepts, theories, frameworks, approaches, principles, methodologies, and models to understand, analyze, characterize, convey, and manage or govern risk (Aven, 2012, Aven and Zio, 2014).

"Safety" refers to the absence or reduction of hazards (Möller, 2012). A typical method of guaranteeing system safety is to identify and eliminate the causes of an accident as soon as it happens and to repeat such efforts (Ham, 2020). This approach can also be called a reactive approach (Dallat et al., 2018). With the advancement of industrial systems evolving integrated control and advanced safety systems, complex operation and shutdown sequences management of risk have become more challenging (Macdonald, 2003). A significant issue consistently pointed out in the literature and investigation reports is that the premises of current practices are too narrow and ill-adapted compared to the behaviors of complex systems (Årstad, 2019).

Understanding the risk of a process system implies understanding how a comprehensive socio-technical system functions and how a business evolves and adapts to its dynamic environment. Before an accident, the emergent nature of risk must be considered to realize the system's complex behavior (March, 1994, Weick and Sutcliffe, 2001). Current practices lack appropriate comprehensive approaches and methods to cover the complexity and dynamic nature of the system. The difficulty remains finding what is missing due to blindness (Årstad, 2019).

Based on the existing limitations, Guarnieri et al. (2019) advise taking a dynamic approach to industrial risk analysis in four complementary stages: design of a dynamic model and simulation of system behavior, comprehensive failure analysis, comprehensive simulation of the consequence of failures, and testing of prevention and protection methods. Other researchers (Varde and Pecht, 2018, Frank, 2010, Cox, 2009) also advise including dependent events and complex interactions during the system's risk assessment. The characteristics of modern automated systems have created the necessity for further research on improving risk management approaches. The motivation of the thesis is to improve the existing methods used in risk management.

1.1.1 System complexity, a high degree of integration, and uncertainty

Using more digital control units, network controllers, and automated workflows have resulted in higher system integration and coupling. The consequences of a single choice potentially may have far-increasing effects. In a system, complexity introduces uncertainty in two ways. First, complex systems are difficult to envisage and comprehend, so the likelihood of effectively satisfying safety requirements decreases as the system becomes complex. Second, it is challenging to design and maintain interactions and interfaces inside the system if any components have been changed. Changes in complex systems may have unfavorable consequences (Kamrani and Azimi, 2011).

Decision-making in risk management is subjected to two types of uncertainty. One stems from randomness. The other is the uncertainty that results from knowledge imperfection. If the analysts do not fully understand how systems behave and fail; thus, having imperfect knowledge of the systems encounters difficulties in analyzing risk. Knowledge imperfection is a natural aspect of a complex and dynamic environment. It makes analysts perplexed when distinguishing between alternatives.

1.1.2 Rate of technological change and scale

Changes in technology happen at a breakneck speed these days. Because of the rapid evolution of technological capabilities, projects may experience uncertainty in selecting the appropriate technical solutions. If managers establish systems, they must also decide on technology (Kamrani and Azimi, 2011). Unsurprisingly, unknown risks may be introduced if novel solutions are not sufficiently evaluated before implementation. The scale of industrial installations is also increasing, increasing the probability of significant scale accidents. Low probability accidents should also be given importance, and actions should be taken accordingly to accept operation.

1.2 SYSTEM PERSPECTIVE IN PROCESS SAFETY AND RISK MANAGEMENT

From 1970 till the 2000s, system-oriented analysis and techniques increasingly became a subject of safety management studies and contributed to initial efforts to establish concepts and strategies of system safety management (Grose, 1971, Hammer, 1971, Pope, 1971, Redmill et al., 1999, Roland and Moriarty, 1990, Levenson, 1995). Rasmussen (1997) advises that a system-oriented approach based on control theory, including organizational, management, and operational structure, should be created due to the inadequacy of existing accident models for modern sociotechnical systems. The author views risk management as a control problem in a sociotechnical system, where unwanted consequences arise due to loss of control of physical processes. Safety depends on the system's ability to control these processes and avoid or reduce consequences causing harm to assets, people, or the environment.

Many other researchers have also combined system engineering (SE) approaches in risk management. Cameron et al. (2005) have used various SE concepts, such as socio-technical factors, complex interactions, vulnerability model, and dependent failures in different risk management phases and hazard identification and consequence analysis. Kamrani and Azimi (2011) have shown how risk and uncertainty can be managed with the help of various risk assessment methods for multiple systems using SE perspectives.

Noteworthy progress toward the process safety field is made by modeling potential accidents using the SE concept. The accident model relates the causes and effects of events that lead to accidents. Accident models seek to explain why an accident occurs and how it occurs. Accident modeling and analysis form the basis of strategies that should be followed to avoid an accident, ensuring the system's overall safety. An example of such works is the theory of normal accidents (Perrow, 2011). Perrow claims that some socio-technical systems have the properties to lead to accidents naturally. He identifies two important system characteristics that make complex sociotechnical systems prone to significant accidents. Two characteristics are interactive complexity and tight coupling. Even if the normal accident theory asserts that accidents are inevitable, it does not mean that nothing should or cannot be done for them. Perrow (2011) concludes that what is needed is an explanation based on system characteristics in accident analyses.

The theory of high-reliability organization (HRO) was developed partly due to the challenges faced by the normal accident theory (LaPorte and Consolini, 1991). Another background for the evolution of the idea was the observation that several complex, high-risk organizations (e.g., aircraft carriers, nuclear submarines, traffic control systems) had been operated for decades without any accidents. The fact implies that the normal accident theory could not be entirely correct, and it is possible to prevent severe accidents by effectively managing organizational processes and practices. The HRO perspective focuses on being initiative-taking, predicting, and avoiding potential dangers as early as possible. A central risk reduction strategy is to build organizational redundancy. This strategy requires that enough competent personnel be available to achieve overlapping incompetence, responsibilities, and possibilities for observation.

Leveson (2004) presents the idea of STAMP, which is an accident causation model based on control theory. It investigates the causes of human performance and component failure due to inadequate control actions. Constraints, hierarchical layers of control, and process loops are the three main components of this model. In this model, accidents are investigated by examining why the existing controls failed to prevent or detect the hazards and why these controls are insufficient in imposing the necessary system safety restrictions (Leveson, 2011).

The functional Resonance Analysis Model (FRAM) is developed to include variability in system performance and complicated interactions between system elements (Hollnagel, 2017). It has been effectively used for accident investigation and risk assessment (Belmonte et al., 2011, Bjerga et al., 2016, de Carvalho, 2011,

Fukuda et al., 2016, Smith et al., 2017). It helps analysts comprehend the accident process and assess potential scenarios without assuming any accident model.

The FRAM model's basic unit is a function (task) with six aspects: input, output, time, control, preconditioning, and resources. The core of the FRAM model, however, would be the relationship between the functions that comprise a system. The five characteristics of each function (Input, Time, Control, Preconditioning, and Resources) affect the performance of that function's output (Ham, 2021). The performance variability of output is propagated in other functions and resonates throughout the system as performance variability affects others, and when two or more performance variability get combined, they create an unexpected outcome. Thus, the FRAM model helps understand an accident's occurrence and assess performance variability.

Bristow et al. (2012) developed a method for risk modeling and managing catastrophic system failures. The key feature of the model is the participation of multiple interacting institutions, for example, government, industry, international organizations, and research institutions, to define the perception of risk in describing scenarios, consequences, and probabilities.

Works toward system-based risk evaluation and management have been done in various fields. However, in the chemical process and oil-gas industry, works are rare. The thesis focuses on filling up the knowledge gap. The author finds a gap in applying the SE perspective, especially in several risk management tasks, e.g., assuring inherent safety of the system, SE-based performance indicator development, and hazard identification. The author thus focuses on these specific areas.

1.3 KEY RESEARCH QUESTIONS

Various accidents have been reported in the process industry from time to time, resulting in severe social and economic impacts. Risks arise from complexity, ambiguity, and uncertainty, posing a challenge in understanding and managing an unwanted event's risk. While managing risk, determining cause and effect relationships is challenging due to multiple interactions of system components and features of automated systems. The present challenges and strategies for improving a safety management system are shown in *Figure 1*

Implementing risk management for an automated system, decision-making, and forecasting significant accidents have become challenging.; the research advises strategies to improve safety implementation based on the identified challenges (*Figure 1*). The study's primary goal is to develop risk management approaches using a system perspective to help decision-makers manage the safety of automated process systems. The main aim is broad, and several research paths would fit it. The research questions are developed from the practical challenges and theoretical background described in sections 1.1 and 1.2.

The following research questions are eventually developed for this thesis:

RQ1. *Are present hazard identification methods adequate for complex systems? How can they be further developed for better risk management?*

The topic of hazard identification is chosen as it is a critical step of any risk management process. If the hazards can be identified early, mitigation measures can be implemented accordingly. There are various hazard identification methods in the industry, for example, failure mode, effect and criticality analysis (FMECA) (Bouti and Kadi, 1994), Hazard and Operability study (HAZOP) (Crawley and Tyler, 2015), and What if (Khan and Abbasi, 1998a). Present research raises questions about whether these existing methods are sufficient for complex systems.

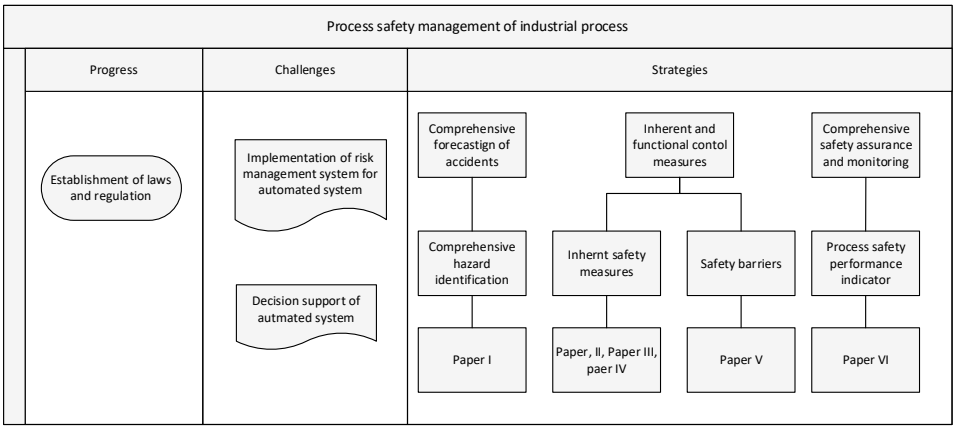


Figure 1: Progress, challenges, and strategies for improvement in the risk management

RQ2. *How can the assessment method of inherently safer design be improved?*

Inherent safety is the most proactive risk management strategy (Khan and Amyotte, 2002, Amyotte et al., 2007). Defining inherent safety, developing the principles of inherently safer design, and establishing the assessment of inherently safer methods have taken much effort in academia and industry. However, those methods need to be revisited to include the complexity and features of the modern automated system. The research raises the question of the present limitations of inherently safer design and how the methods can be improved based on the system perspective.

RQ3. *How can safety barrier allocations be improved in automated systems?*

Defining and implementing barriers is essential to ensure safety in the process. Barrier systems can be physical, technical, or operational. It is vital to check barriers' attributes, such as functionality/effectiveness, reliability/availability, response time, and robustness. It is essential to know that a comparable level of risk reduction has been achieved in compliance with existing standards for highly hazardous systems

in the petrochemical industry. This research raises the question of how the barrier strategy and allocation method be improved considering the features of the automated system.

RQ4. *How can improved SPIs be established to ensure better risk management?*

The last step of risk management is risk monitoring to become aware of the plant's safety performance. The primary goals of safety indicators are to monitor the state of safety in a system, inspire action, and equip decision-makers with the knowledge they need to know where and how to act (Osmundsen et al., 2008). The main challenge is identifying indicators that allow management to work on the early warnings and respond within a suitable timeframe (Hale, 2009). This research questions whether existing SPI development methods are effective enough and how they can be developed to improve risk management.

1.4 OBJECTIVES

The thesis discusses improved methods using system perspectives so that it becomes possible to make better decisions for automated systems; the main objective is as follows:

Improvement of risk management of automated systems using system perspective

The following sub-objectives are set to achieve the main objective considering the research questions stated in section 1.3 and to answer the research questions. Sub objectives are as follows:

Sub-objective (i)	Identify and evaluate existing methods of hazard identification and development of process using SE approaches
Sub-objective (ii)	Identify and evaluate existing methods of inherent safety evaluation and challenges in the industrial application; develop a framework for inherent safety evaluation for the system
Sub-objective (iii)	Development of improved barrier allocation method using SE concept
Sub-objective (iv)	Evaluation of existing methods for developing performance safety indicators and development of SPIs applying the SE method

1.5 SCOPE AND LIMITATIONS

The present research focuses on process safety, risk management, and related issues. The thesis discusses improved methods with the help of a SE perspective so that it becomes possible to make better decisions for automated systems; however, decision-making itself is not the focus. Risk management is an extensive compilation of issues involving risk communication, assessment, treatment, and monitoring. Risk assessment covers risk identification, analysis, and evaluation. Due to time

constraints, it is decided to explore four specific critical areas of risk management: hazard identification, inherent safety, barrier management, and safety performance indicators, which cover part of risk identification, risk evaluation, treatment, and monitoring.

Methods are improved or developed considering risk and safety issues relevant to the chemical and oil-gas plants. Although risk management covers all kinds of accident risks, including minor and major accidents, present research only considers process-related major accident risks. Environmental, occupational health, and safety risks are kept out of the scope of the study.

The plant's design, installation, and the operation go through several distinct phases, e.g., feasibility study, concept selection, detailed engineering, implementation, and operation. The ideas and case studies used for inherent safety focus on the conceptual stage. Case studies for other covered topics explored methods to improve safety issues, applicable for both design and operational phases.

The primary audience of the thesis is researchers and practitioners who have basic knowledge about process safety and risk management and are motivated to use them for better decision support. Present work can be characterized as applied, qualitative and analytical. It seeks to develop concepts for the process and petroleum industry to meet research questions raised, justifying attention to issues.

1.6 THE LAYOUT OF THE THESIS

This Ph.D. thesis consists of two main parts:

- Part I- The main report contains the background, research challenges, and questions leading to the research objectives with defined limitations. In addition, this section describes the theoretical knowledge and the research method and design. Finally, this part presents and discusses the main results from the papers with concluding remarks and directions for future research.
- Part II – Papers: the second part is a collection of papers presenting the contributions of this research. In total, four journal papers and two conference papers are included.

The first chapter of part I discusses the context and background for the Ph.D. study and the work's objective, scope, and limitations. The framework of the thesis is also defined. Chapter two summarizes the existing theories and knowledge gaps for risk management on selected issues (hazard identification, inherent safety, safety barriers, safety performance indicators) and explores the challenges concerning the implication of theories in practical applications. Chapter three includes a brief evaluation of the research process and assesses the quality of the research. Chapter four presents the main results and discusses detailed scientific contributions and contributions to practical applications. Chapter five presents overall conclusions and proposes ideas for further work.

2 LITERATURE REVIEW

The motivation behind a theoretical literature review is twofold. The first is to shape the research questions by understanding state of the art and revealing challenges. The second is to identify methodologies to develop answers. The present section reviews existing literature on selected topics discusses the concept of established methodologies, highlights the limitations, and discusses the need to improve the methodologies.

2.1 USE OF SYSTEM PERSPECTIVES IN RISK MANAGEMENT

Knowledge gaps remain in understanding the system in detail, identifying and quantifying consequences in precise and assessing probability (Bristow et al., 2012). Strategic interaction among multiple elements plays a vital role in managing risk in a system of systems. As the number of causes, effects, and feedback loops in the system increase, the system's behavior becomes more difficult to predict. Moreover, multiple interacting participants may produce emergent behavior, and their effects on the system behavior can be unpredictable. Increasing complexity presents a significant challenge to risk experts because the system's functioning is harder to understand (Kamrani and Azimi, 2011). SE ensures that the system's components work together to achieve the overall goal and, in turn, meet the needs of the consumers and other stakeholders who will acquire and utilize the system (Haskins et al., 2006).

Various researchers have applied system perspective and SE tools for systems risk analysis and accident analysis. Rasmussen (1997) advises that risk management should be modeled as a cross-disciplinary study, and risk management should be considered a control problem. The control structure should involve all levels of systems for each hazard. All relevant controllers, objectives, performance criteria, control capability, and information should be identified for a particular hazard source. According to the author, a system-oriented approach must focus on functional abstraction rather than structural decomposition.

McLucas (2003) discusses how a system dynamic model can improve decision-making in risk management. Cameron et al. (2005) and Garvey (2008) present a method using a system model for risk management. Instead of the traditional risk management view, Cameron et al. (2005) advise adopting risk management throughout the system's lifecycle, considering sub-systems and their boundaries, and integrating system thinking for effective risk management. Van Scyoc (2008) has applied the TRIZ theory of inventive problem solving to check its effectiveness in safety improvement. TRIZ is built from the concept of idealism, which is that technical systems must be developed toward eliminating harmful effects while leaving nothing but the beneficial effects of that technology. Fundamental thirty

parameters are identified as features of inventive problems. Forty principles represent the various problem solutions that resolve contradictions. TRIZ can define a problem in technical terms, recognizing that the resolution of one problem may introduce another.

Reniers et al. (2009) advise cluster safety procedures for improving the process safety management of a big organization. The cluster approach helps safety improvements of companies situated within the same large industrial area. In clustered approach, three kinds of accidents are considered: accidents occurring to an individual, accidents occurring to the organization, and accidents occurring in clusters of organization. It develops a loop safety structure that gives safety recommendations for factory, plant, and cluster levels. Cluster organization consists of four levels of analysis, including humans, subsystems, collection of systems, and the organization itself. Involved stakeholders at each level are identified to check the effect of the action on safety. The cluster model can prevent domino events more effectively.

Nicholas (2017) uses the SE concept in risk management with various practical applications. According to the author, the primary method of preventing accidents should be through a comprehensive and systematic approach to safety management. Garbolino et al. (2019) discuss system concepts and system modeling for safety and risk management. The authors advise assessing system dynamics and simulating system behaviors to ensure safety.

STAMP accident model (Leveson, 2004) incorporates analysis of human factors, software, new technology, organizational design, and safety culture, all relevant to today's complex systems. Nowadays resilience-based accident analysis model is attracting the attention of researchers. Many researchers (Niskanen, 2018, Rosness et al., 2010, Pasman, 2015, Steen and Aven, 2011, Woods and Wreathall, 2003, Ranasinghe et al., 2020) have worked on the relationship between accident occurrence with risk control based on resilience. A system is resilient if it can modify its functioning during or after changes and disturbances, maintaining essential operations under-predicted and unforeseen conditions. A key aspect of resilience is that systems should also be robust against all possible unwanted events. In this approach, safety is based on four fundamental principles: anticipating, recognizing, evaluating, and controlling.

Another recent direction of work is dynamic risk management (Paltrinieri, 2016, Paltrinieri et al., 2014, Grøtan and Paltrinieri, 2016). Dynamic risk management focuses on continuous information from early signals of risk related to the event. This method helps to identify and assess probable atypical accident scenarios involving the materials, equipment, and location under consideration and capture available early warnings or risk concepts. A dynamic risk management framework can potentially update the overall risk picture by deriving risk-related knowledge from resilient functioning. The present research takes a step to focus on some issues of safety management from a system perspective, considering the prospects of system perspective and system-based engineering.

2.2 RISK MANAGEMENT STRATEGIES COVERED IN THE THESIS

2.2.1 Hazard identification techniques

Most activities conducted in the process industry involve a certain level of risk. Hazard identification is a vital step in risk management because if the risk is not identified correctly, it will be outside of the rigor of the risk management process, leading to the non-identification of preventive measures for implementation and communication to prevent harm (OSHA, 1983). Therefore, the facility should develop and maintain formal processes to identify hazards in operations and maintenance. Identifying hazards should combine reactive, proactive, and predictive approaches (Bartulovic, 2021). Adopting a system safety method will allow analysts to shift their focus to a more detailed strategy for identifying and prioritizing hazardous events upstream.

Various hazard identification methods have been discussed in the literature (Crawley and Tyler, 2003, Ericson, 2005, Wells, 1997), and various techniques have been used in the industry, for example, safety audits (Lees, 2012), checklists (Rausand, 2005), hazard indices, Dow index (Gupta et al., 2003), Mond index (Lewis, 1979), what if analysis (Burk, 1992), event tree analysis (ETA) and fault tree analysis (FTA) (Freeman et al., 1966), bowtie method (Khakzad et al., 2012), hazard and operability studies (Crawley and Tyler, 2015, Singh and Munday, 1979), FMECA (Bouti and Kadi, 1994), preliminary hazard analysis (Kavianian, 1992), hazard ranking method (Haness and Warwick, 1991) and others.

A safety audit or hazard checklist identifies health and safety hazards by examining conditions or practices in the workplace (Saunders, 1992). However, there remains uncertainty about whether the method could identify all hazards, accident scenarios, and consequences. The method depends on the analyst's assumption at the beginning of the procedure and can be used as a preliminary hazard analysis of a straightforward known system to the experts.

ETA follows an inductive procedure that shows all possible outcomes resulting from an initiating unanticipated event, considering whether safety barriers are functioning or not (Ramzali et al., 2015). Multiple failures and system weaknesses can be identified by this method. The limitations are that ET addresses only one initiating event at a time. Success and failure probabilities are difficult to find. ETA is not efficient in analyzing multiple co-occurring events. All events are considered independent here, which may not be accurate in real life. Using binary logic (yes or no) may not be feasible in real-life accident scenarios where common mode failure, human errors, and adverse weather conditions play together (Mosher and Keren, 2011).

FTA investigates how a specific top event, abnormal condition, or failure can be traced back to its source. FTA demonstrates a logical relationship between events and factors that causes failure (Lee et al., 1985). It helps to understand the weaknesses in the design quickly. However, the entire method is time-consuming and expensive. FTA cannot consider the time sequence of failure or an asset’s useful

time. One specific top event is examined at a time. Additional FTA is developed to analyze other top events. Analysts may ignore failure modes and overlook common cause failures caused by a single problem that affects two or more safeguards (Lee et al., 1985). FTA also assumes all events as independent (Fussell, 1975). FMECA can identify failure causes such as component interactions or software faults, but it does not consider the operational context (Stamatis, 2003).

As technology advances, conducting hazard identification has become increasingly difficult (Jensen, 2018). The present research focuses only on two hazard identification methods, HAZOP and STPA. The HAZOP technique is widely utilized in the process sector and is the foundation of many companies' hazard identification systems (Baybutt, 2015). The HAZOP was developed in the 1960s to analyze chemical process systems (Crawley and Tyler, 2015). Its success led to the method being extended to make it suitable for other systems and complex operations, including mechanical and electronic systems, procedures, software systems, organizational changes, legal contract design, and review. It systematically examines a product, process, procedure, or system to identify hazards and operability issues. The method systematically examines how each design part responds to critical parameter deviations. Guidewords are used in association with parameters to indicate deviations. The guidewords can be customized, or generic words can be used that encompass all types of variations.

A multi-disciplinary team conducts HAZOP execution in workshops led by an independent HAZOP facilitator, and findings are formally recorded on worksheets by a HAZOP scribe/secretary. Experts from all disciplines must meet face to face to execute a HAZOP and check for deviations. Feedback from all discipline experts, such as electrical, automation, instrumentation, software, and process, is considered when determining the deviation. A process flow diagram, pipe, and instrumentation diagram (P&ID), or other information that exposes the design purpose is required for the investigation (Toghraei, 2019). HAZOP has been modified to give particular focus to environmental effects (Choi and Byeon, 2020) or systems other than process vessels (Li et al., 2014) or computer-controlled plants (Andow et al., 1991) or human interactions (Ellis and Holt, 2009). The procedure has been discussed in many works of literature and guidelines (Grossel, 1993, Lawley, 1974, Crawley and Tyler, 2015, Redmill et al., 1999, Macdonald, 2004, IEC, 2001, Kletz, 2018).

The strengths of HAZOP are that the method is systematic, comprehensive, widely applicable, easily customizable for various applications, and guidance is available in abundance. However, it does have some limitations. One such limitation is in the scope evolving from assumptions. The method presupposes that the design is completed according to the necessary codes in its original form. Thus, it is expected, for example, that the design accommodates pressures under normal operating conditions and desired relief situations. HAZOP aims to identify pressure deviations that may not have been anticipated (Mannan, 2014).

Another limitation is not meant to be there or desired but is built into the approach. For example, it is not well-suited for dealing with spatial factors related to plant

layout and the consequences. Thus, this is not a replacement for good design (Mannan, 2014). HAZOP analysis concentrates on single events rather than probable combinations of events (Ericson, 2005). Other limitations are that it can be time-consuming, expensive, requires experienced practitioners, and depends on the scenario description and system-level analysis (Kletz, 2018). Control Hazard and Operability Study (CHAZOP) is developed to identify potential hazards and operability problems in control and computer systems. Although there are several CHAZOP techniques, none have been certified as an acceptable engineering practice. CHAZOP is believed to have four technical shortcomings: ambiguity, incompletion, illogic, and redundancy (Hulin and Tschachtli, 2011).

In the present research, considering the limitations of HAZOP, an alternative hazard identification method, STPA, is chosen to check whether STPA can overcome the limitations of HAZOP. STPA is a recently used hazard identification technique based on a SE accident model, STAMP (Leveson, 2011). STPA has been applied in various industries, for example, aviation (Karanikas and Abrini, 2016, Plioutsias and Karanikas, 2015), automotive (Abdulkhaleq, 2013), space (Nakao et al., 2011), nuclear power (Rejzek and Hilbes, 2018), chemical industry (Chahal and Mohammed, 2019, Hoel, 2012). However, the application of STPA in the process industry is scarce except few earlier works (Hoel, 2012, Chahal and Mohammed, 2019).

Considering the scarcity of STPA application in the process industry, it is decided that STPA should be applied in more cases in the process industry, and a comparative study between HAZOP and STPA should be conducted. Comparing STPA and HAZOP is also scarce except few earlier works (Budde, 2012).

2.2.2 Inherently safer design

Inherent safety is considered the most effective risk management strategy. However, applying inherent safety in practice is challenging (Moore, 2003). The pioneer of the concept of inherent safety, Trevor Kletz, provided good examples of application in the process industry through his extensive work (Kletz, 1985, 1991, 1995, 1999, 2003, 2010). CCPS also proposes inherently safer designs based on corrective actions (CCPS, 1993).

Inherent safety indices for assessing, ranking, and selecting inherently safer process alternatives have improved significantly in recent decades (Gao et al., 2021, Abidin et al., 2018). Inherent safety indices establish a set of numerical scales to compare alternative designs concerning how well they possess inherently safer design principles. The method considers selected parameters for comparing the inherent safety of a design, such as inventory, temperature, pressure, yield, toxicity, flammability, and explosiveness (Edwards and Lawrence, 1995, Heikkilä, 1999, Palaniappan et al., 2002). In the Numerical Description Inherent Safety Technique (NuDIST) method (Ahmad et al., 2014), the index is developed through logistic equations to eliminate the shortcoming of subjective scaling.

Indices like ISI (inherent safety index) and NuDIST do not consider interactions of various parameters in the system (Gao et al., 2021). The gap was attempted to be fulfilled by other indices, e.g., process safety index (Shariff et al., 2012), exergy inherent safety index (Li et al., 2011), and comprehensive inherent safety index (Gangadharan et al., 2013). These methods incorporated the compounding effect of materials and equipment. Determining the Optimizable Fuzzy Inherent Safety Index (OFISI) follows a systematic approach to optimize safety levels besides inherent safety assessment (Vazquez et al., 2019). Equipment characteristics and performance evaluation are addressed in the Inherently Safer Process Equipment Index (Athar et al., 2019) and Equipment-based Route Index (Athar et al., 2020). Equipment performance is also considered in the Integrated Inherent Safety Index (I2SI) (Khan and Amyotte, 2004).

The risk-based matrix is developed considering main accident scenarios regarding their severity of consequence or likelihood of occurrence (Jafari et al., 2018, Khan and Abbasi, 1998b). Risk-based approaches can be considered preliminary risk assessment (Shariff and Leong, 2009, Shariff et al., 2012, Rusli and Shariff, 2010), although they are very similar to quantitative risk analysis (QRA). QRA is a formal and systematic method for determining the probability of loss and other associated hazards by using objective data. A QRA will emphasize the accident scenarios that significantly impact overall risk, including the consequences and elements that cause and control the accident. The assessment results demonstrate that the facility meets acceptable standards and that risks are kept as low as reasonably practicable (ALARP).

Risk-based inherent safety indices and QRA can be used in the preliminary engineering phase, while QRA needs detailed process information applicable in detailed engineering phases. The risk-based safety index (Rathnayaka et al., 2014) integrates the reduction of both consequence and probability of accident occurrences by applying inherently safer design principles in the process design life cycle.

Several assessment approaches have been developed to evaluate the inherent safety prospects of specific process hazards or undesired outcomes. The Process Route Index (Leong and Shariff, 2009), for example, is designed to assess the explosiveness degree of processes. The level of process explosiveness is seen as a measure of the system's intrinsic safety. A Toxic Release Consequence Analysis Tool (TORCAT) is designed to assess the risk of toxic release (Shariff and Zaini, 2010). The toxic release is considered an indicator of the inherent safety of the system here. The process stream index (Shariff et al., 2012) is developed to calculate the inherent safety of process streams influencing the explosion.

A graphical heuristic method is proposed by plotting parameters associated with inherent safety concerns for each step of each process option (Gupta and Edwards, 2003). Graphical methods aim to present safety levels through easy-to-understand tables and figures (Gao et al., 2021). In the graphical technique (Ahmad et al., 2015), authors used logistics functions to determine root cause analysis of hazards posed to the process.

Many inherent safety, health, and environment (SHE) studies have been developed to eliminate or reduce SHE hazards in an inherently safer way. SHE approaches focus on inherently safer and more environmentally benign process routes. Some pioneering works are Process Route Healthiness Index (Hassim and Edwards, 2006), and Inherent Environmental Toxicity Hazard Index (Gunasekera and Edwards, 2006). Several inherent safety-based indices, e.g., inherent risk assessment tool (Shariff et al., 2006), Inherent safety index module (Leong and Shariff, 2008), and Inherent risk assessment (Shariff and Leong, 2009), have been developed by combining process simulators such as Aspen HYSYS (HYSYS, 1995) with the developed index.

Song et al. (2018) present a framework to assess inherent safety to enhance the sustainability of chemical process design. Summers (2018) discusses how the design of automated systems can be improved using inherent safety principles. The author also emphasizes that combining all accident prevention strategies (active, passive, inherent, procedural) is essential for a comprehensive safety management system. The reason is to deal with all potential hazards in the process plant and reduce the risk to the lowest possible level, known as a maximum acceptable risk, to ensure a sustainable, cleaner chemical process.

Multitarget inherent safety index (Crivellari et al., 2021) ranks inherently safer alternatives in the early design of offshore oil and gas production systems. An array of key performance indicators is proposed based on the consequences of potential accident scenarios concerning different effects on offshore oil & gas production installations. The method evaluates and ranks the various hazard sources, considering the specific features of offshore facilities such as multi-layer layout, high congestion, and others.

Some methods, e.g., Dow Fire and Explosion Index (AIChE and Dow, 1987) and Mond index (Lewis, 1979, Li et al., 2008, Tyler, 1985), are not usable in the early stage of the process design (Rahman et al., 2005). The results of these procedures are difficult to interpret. All aspects of inherent safety, e.g., layout, complex interaction, and all inherent safety guidewords, cannot be considered by those approaches. Additional rigor, accuracy, and precision are often required to assess safety measures' impact on the values of hazard indices (Khan et al., 2001). Some indices (Dow, Mond) showed no value change for an equipment change. When applied to different life cycle stages, I2SI is inflexible. Another limitation of existing parameter-based approaches (e.g., ISI, SHE) is that they do not consider the interaction between distinct factors. They are not adaptable enough to accommodate newly available data. Parameters defined for one sort of industry may not be applicable to another.

Distinct types of hazards may become dominant for various applications. Prototype Inherent Safety Index (PISI) (Lawrence and Edwards, 1994, Lawrence, 1996) and ISI (Heikkilä, 1999) describes inherent safety based on a few specific types of hazards. Another problem is that they (e.g., PISI, ISI) have sudden jumps in the score value. The index-based approach does not assist the user in thoroughly

understanding the hazards that evolved in each processing path because it does not address the actual cause of risks.

Another problem is the dimensionality problem (Gupta and Edwards, 2003). Adding parameters of different dimensions like temperature (◦C), pressure (atm), inventory (t), toxicity (ppm), and comparing the summed value may become unacceptable scientifically from the chemical engineering point of view. Risk-based approaches are helpful because the overall goal is to reduce risk. Risk can be compared for distinct designs and can be modified accordingly. The process route index helps rank between different chemical process routes. However, it only considers explosion potential.

The industry has faced problems implementing these methods due to a lack of expertise. A second reason is the complexity of implementing them in practical cases. Also, industry personnel may not be interested in using any risk evaluation tool besides QRA, as there is no regulatory requirement, and the industry has used QRA for a long time. Additional cost, time, and need for expert resources may discourage them from using such a tool. Another reason is the lack of information to set the parameter values. Index values (e.g., chemical interaction, correction) are not readily available (Rahman et al., 2005). Most risk-based indices methods are applicable later in design stages and require detailed data and time. It is difficult to use them at the early design stage when there is enough leverage to make changes in plant design.

Managing risk means assuring the safety of the system in a system world. Ade et al. (2018) study the impact of intrinsic safety principles on system reliability in process design. This methodology assesses the probability of higher risk because of decreased system reliability and underlying design philosophy. Recent research has been directed toward assuring inherent safety from a system perspective. In this thesis, further research has been conducted, considering the chemical process system's vast nature, and relating many risk factors. The research works further to fill the gap in selecting safer materials and equipment.

2.2.3 Safety barriers

Several safety standards have been developed on risk control and safety barriers, such as IEC 61508 (2010), ISO 13702 (2015), and ISO 28781 (2010). The generic standard IEC 61508 (2010) translates safety system requirements into barriers under common cause and dependency failures. IEC 61511 (2003) and ISO 13702 (2015) also demonstrate the importance of safety barriers to reduce the risk of accidents. The safety barrier concept, classes, and performance criteria are clarified by Sklet (2006) and Hollnagel (2016). Requirements for safety barriers to prevent various accidents can be understood using multiple models such as the bowtie diagram, Swiss cheese model, ETA, and energy barrier model (Kang et al., 2009). Proactive barriers are upstream of accidental events, while reactive barriers are downstream (De Dianous and Fievez, 2006, Sobral and Soares, 2019).

Bowtie analysis has been widely used in numerous literature as it is straightforward and concise. It demonstrates risk controls by placing barriers in scenarios. The relationship between sources of risk, control, escalation factors, events, and consequences is illustrated by a bowtie diagram (Rausand, 2011). The whole range of initiating causes can be displayed with their existing controls. Bowtie diagrams have the drawback of being predicated on the notion that a linear series of events create accidents. When several causes are linked in complicated ways, the bowtie is insufficient, and analysis needs scenario identification, including coupling effects of system elements. Another drawback is that the risk controls are not provided in a time or process-oriented manner (Aust and Pons, 2019).

To describe critical barriers and determine their effectiveness, Sklet and Hauge (2004) constructed an accident scenario that can allocate barriers and analyze the effect of the failure of barriers. Quantification of the scenarios is a challenge of this model. Researchers have used various methods to assign safety barriers and find how effectively they can prevent accidents. Janssens et al. (2015) proposed a metaheuristic solution to assist decision-makers in determining where safety barriers should be placed and how to limit the consequences of an accident that causes domino effects. The concept is to delay the failure time associated with a domino event of a chemical plant.

Xie et al. (2018) applied an extended bowtie model to identify barrier requirements in a system. It is seen that various types of barriers can be identified by using the extended bowtie model, e.g., barriers against effects of the root cause or coupling factors affect or cascading failure. The extended bowtie model can study the effects of different safety barrier strategies and the reliability of independent barriers. Groot (2016) advises that combined with incident analyses on barriers, the bowtie method can be adapted to understand, monitor, and analyze barrier performance factors.

A combined method of bowtie and LOPA is used by Neto et al. (2014). The bowtie can identify required barriers to prevent an accident. It explains how an accident can be avoided but does not measure the system's risk or identify the uniqueness of barriers. LOPA is used to identify protections that fit the Independent Protection Layer (IPL) (Willey, 2014). A computerized system collects real-time data from operational systems to provide a notion of the platform's safety functions. The integrity is monitored using a series of queries from the unit's management elements concerning the instrument or equipment related to each layer.

A risk-based inspection approach Synergy Plant RBI is applied to manage safety barriers by Hosseinnia Davatgar et al. (2021). The authors modified the Synergy Plant RBI model to consider management performance by bowtie analysis and adjusted the confidence level of safety functions accordingly. The study shows that technical and management aspects are feasible for managing safety barriers.

Based on facility-specific risk pictures and generic performance requirements, Jansen and Firing (2016) establish specific barriers or safety strategies to evaluate the technical integrity of Statoil’s oil and gas production and processing plant. The concept is built on a generalized bowtie model where the top event is an accident

such as a blowout or ignited risk. A three-stage process is proposed to ensure the performance of barriers. The first stage is to apply the maintenance concept to outline requirements for rest and overhauling equipment and system. Secondly, regular evaluation of technical integrity and visualization. Thirdly regular technical condition monitoring after several years.

Technical integrity is evaluated at three levels: equipment/ sub-system level, area, and facility perspective. Non-technical barriers are not directly included in the evaluation. It is known that 60-80% of barrier breaches leading to significant accidents are non-technical, such as lack of competence or risk understanding, quality of procedures or how they are followed, and many more. HSE work focuses on non-technical barriers such as HSE campaigns, training, incident reporting, compliance verification, auditing, management supervision, and incorporation of checkpoints in daily work, and work processes are also advised to perform.

Recent works have been directed toward dynamic barrier management (Ahluwalia and Ruochen, 2016, Hosseinniaa et al., 2019, Nelson, 2016, Pitblado et al., 2016). The strategy expresses barrier status in real-time, including direct and indirect indicators of barrier performance using complete information. Inspection, preventative maintenance, audit, sensors, process control, near-miss or incident records, and big data concepts can all be used. Dynamic barrier management provides better safety cheaper than current barrier management methods (Pitblado et al., 2016). The assessment helps the plant identify degraded barriers more swiftly and cost-effectively (Pitblado et al., 2016).

Pezeshki (2020), In his work, used FRAM for barrier management for offshore drilling. His case study highlights the utility of FRAM in the development and maintenance of barrier strategies. The FRAM model is used to combine reactive barrier functions after identifying a threat. Variability-increasing scenarios are discovered. The scenario analysis reveals that variability is enhanced owing to human functions rather than system technical factors. One significant advantage of FRAM is that it may be regarded as an iterative barrier strategy technique in barrier management (Herrera et al., 2010).

Despite many recent works, only a few covers the quantitative evaluation of FRAM and barrier management in a process system using FRAM. The present research explored FRAM to check the adequacy of safety barriers considering the complexity of automated process systems.

2.2.4 Safety performance indicator

Various existing accident theories and models affected the evolution of safety performance indicators, e.g., Heinrich's accident model (Heinrich, 1941), Bowtie metaphor (Nielsen, 1971), Tripod theory (Doran and Van Der Graaf, 1996), and Swiss Cheese model (Reason, 1997). All contributed to the establishment of various models of safety performance indicators. While establishing indicators in the process industry, three accident models contributed: Heinrich's pyramid model, Reason's

Swiss cheese model, and the bowtie model. Risk indicators are also often derived using the QRA model.

After the BP Texas City refinery accident, the UK Health and Safety Executive (HSE, 2006), US Chemical Safety and Hazard Investigation Board (Visscher, 2008), American Petroleum Industry (API, 2010), the Centre for Chemical Process Safety (CCPS, 2012) developed methods for selection of safety performance indicators to monitor and control risk more effectively. HSE (2006) study includes advice for defining, selecting, and implementing process indicators for critical process hazards. They proposed a road map based on British chemical industry practice for management and safety specialists. Instead of relying on failure monitoring (lagging), the risk management system should prioritize the timely detection of weaknesses (leading). The risk control system selects barriers for each scenario based on severe accident scenarios. Finally, each risk control system is linked to lagging and leading indicators, ensuring a two-fold level of assurance (HSE, 2006).

The disadvantage of lagging safety performance indicators is that they only tell how many accidents happened in each period and do not tell how well the organization prevents incidents and accidents. Furthermore, with low injury or accident rates, management may become reluctant to improve the system further. Leading indicators are helpful since they are predictive and allow the company to check its performance. It may, however, be challenging to modify them. They give users information about the impact of the organization's initiatives.

The absence of safety control integration between technical, management, and organizational entities is a significant flaw in today's techniques. The indicator program can only be considered proficient enough if a safety management system can analyze the complete system and its complex interactions, subsystems, and dynamic behavior. For today's automated modern systems, SE tools have been seen as more effective in capturing the dynamic risk of the system (Rasmussen, 1997). Leveson (2014) uses the STAMP model and STPA to identify leading risk indicators.

Valdez Banda and Goerlandt (2018) propose measuring the system's performance using key indicators. The STAMP framework is used to structure a maritime safety management system. The STAMP approach allows for the systematic identification of essential components of safety management that must be in place. This systematic identification is necessary for comprehending the structure of an organization's safety management practices and incorporating a clear trace of these practices across the organizational structure. Two concrete phases have been introduced to aid in the safety management system. The first stage is to establish an identification process for defining critical performance indicators for planning, monitoring, and evaluating the operation of the safety management system. The second stage is developing a performance monitoring method to track, measure, and update the key performance indicators and the safety management system's operation.

The present thesis has developed an SPI program for the LNG plant industry, considering the system-specific characteristics of the indicators. Although Leveson (2014) presents an application of the model for the aviation industry, the present

research has extended the research in this direction for the process and petroleum industry.

3 RESEARCH METHODOLOGY

3.1 RESEARCH APPROACH

'Methodology' refers to methods used in a particular area of study or activity (Oxford, 1989). This section presents several types of research and development activities and their criteria. The kind of research executed in this Ph.D. study is stated, and compliance with the requirements is described in present section. Research is a systematic approach to learning about things that are currently unknown by analyzing occurrences several times and in various ways (Laura and James, 2014). It entails gathering, arranging, and analyzing data to understand a topic or issue better. Research methods are chosen to answer a set of research questions. The research question and the focus on the phenomenon influence the selected research method (Yin, 2011).

Kothari (2004) describes diverse types of research along four axes, descriptive vs. analytical, applied vs. fundamental, quantitative vs. qualitative, and conceptual vs. empirical. The present work is applied, qualitative, analytical, and conceptual. It seeks to develop concepts for the process and petroleum industry to meet the research questions raised, justifying attention to issues. Considering the complexity of automated systems and the wide-ranging safety and risk management topics, understanding the problem is critical and qualitative understanding is more important than quantitative. The effectiveness of safety management stems from a deeper understanding of the system and its complexity. Qualitative approaches enabled an understanding of risk and detailed information about the system.

3.2 RESEARCH STRATEGY

The research entails five main activities (*Figure 2)*:

- Formulation of research questions
- Collect information related to the questions
- Develop/select a model to aid in answering the questions
- Execution of the model with real case studies
- Find answers to the questions

3.2.1 Formulation of research questions

The research questions (*Figure 3**Error! Reference source not found.***) are developed using the author's professional experience and NTNU academic courses. The courses completed at NTNU cover system safety management, risk modeling, model-based safety assessment, and risk influence modeling. These courses guided the author in conducting the research and generated a solid theoretical basis for the project. The author has worked in the Norwegian oil and gas industry for several years. The

challenges faced by the author while conducting projects worked as stimulation to raise the questions as a researcher. The course supervisors, highly acquainted with the work of the industry, provided feedback to the author for the formulation of the questions.

3.2.2 Selection of research method

The research method is based on understanding existing risk management methods and finding the limitations of the models. Limitations of the existing models are inspirations for the questions. The research plan was developed based on the gaps identified from the review. The research papers have presented new concepts and ideas based on the literature reviews and challenges. The developed concepts and theories are based on existing literature, logical reasoning, and critical argumentation.

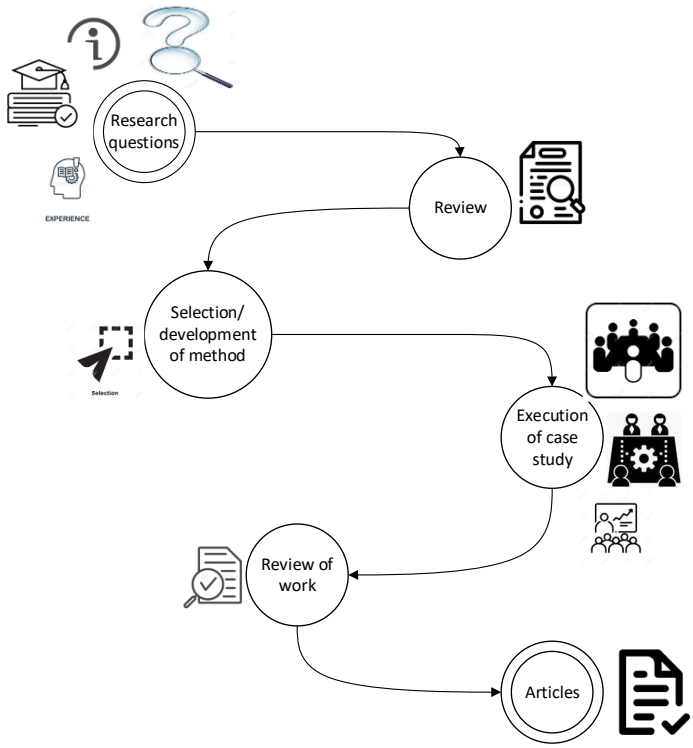


Figure 2: Research process followed in this Ph. D project

3.2.3 Data collection and execution of case study

The current work drew multiple sources of information to answer the research questions. The case study selected is a typical LNG ship-to-ship transfer system. The system information was collected from relevant literature based on the author's

industry experience. HAZOP study of Paper I was performed in a workshop with the company's team members. A series of QRAs, testimonies, and literature reviews are examples of data. The literature review was done online using standard bibliographic databases such as Google Scholar and Scopus.

The chosen or developed methods are evaluated in practical case studies, which show the models' applicability in practical cases. The intermediate results of the research are presented at European Safety and Reliability (ESREL) and Probabilistic Safety Assessment and Management (PSAM) conferences. The conferences provided meaningful feedback for further research and insights into the research trends in the field.

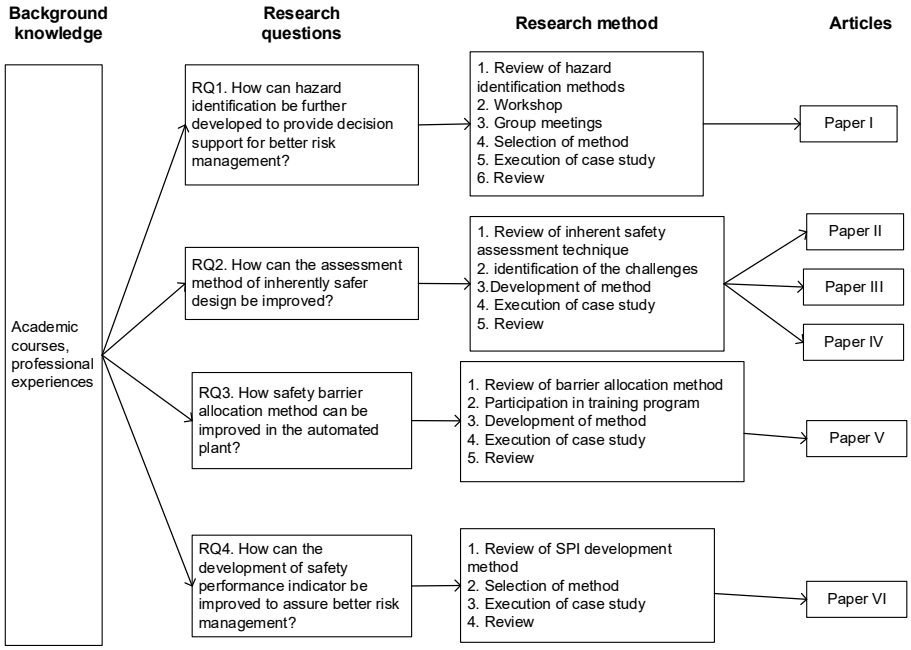


Figure 3: Research strategy applied to conduct the Ph.D project

3.2.4 Review of work and publication of papers

The research conducted during the Ph.D. project integrates the following elements:

- Literature study
- Guidance from supervisors and discussion with co-authors
- Discussions with practitioners from companies and organizations within the relevant sectors
- Presentation of papers at international conferences

- Peer-reviewed paper publications

Six papers included in the thesis have been subjected to peer review through submission and publication in acknowledged journals and international conference proceedings (*Table 1*).

Table 1: Overview of research approach and quality assurance for the papers included in this Ph.D. thesis

Paper	Research approach	Quality assurance
Paper II, Paper III,	Qualitative, Applied	Expert judgment Published in peer-reviewed conference proceedings
Paper I, Paper VI	Qualitative, applied	Test on a real case study Expert judgment Published in peer-reviewed journals
Paper IV, Paper V	Semi-quantitative, applied	Test on a real case study Expert judgment Published in peer-reviewed journals

3.3 QUALITY ASSURANCE

The criteria listed in *Figure 4* are checked to lend scientific credibility to work. The leading quality assurance is via critical reviews from advisors and scientific publications in international journals and peer-reviewed conferences.

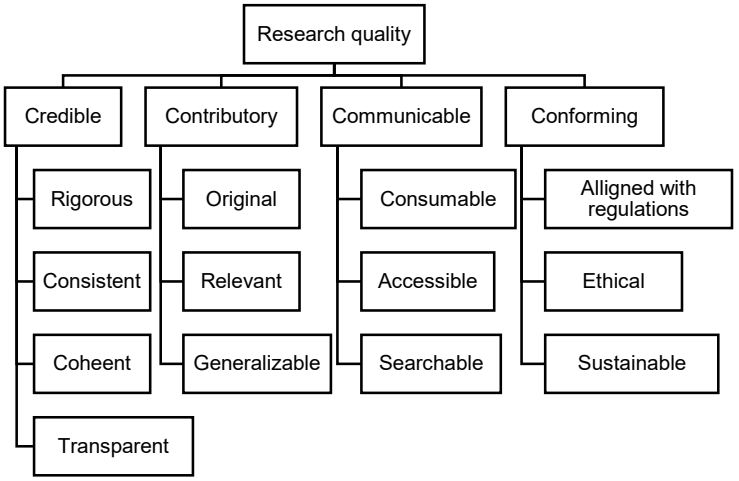


Figure 4: Hierarchy of research quality (Mårtensson et al., 2016)

3.3.1 Credible

The credibility criterion refers to whether the research results are coherent, rigorous, consistent, and transparent. Concepts should be systematically related, and data should be well linked to the developed theory to maintain coherency and consistency (Miles and Huberman, 1994). In the present research, credibility is assured by describing the research process in each study, e.g., the participants and documents that served as data sources, the methods used, and questions asked, and the analytical process. The discussion of the results after each case study is subjective. Other researchers may analyze and interpret the results differently. To keep the rigor, the authors of each paper went through brainstorming during the biweekly meetings. The opinions and observations of each author were recorded carefully. Three papers were presented and discussed at conferences.

3.3.2 Contributory

Contributory refers to whether methods are original and results can be generalized or transferred to other contexts or settings (Trochim and Donnelly, 2001). Findings should be discussed with assumptions to check contributory characteristics. All the conclusions and context of case studies are described in detail to be applied easily in other case studies and settings. To achieve 'generalism', studies should adapt to different application areas and other industries. Details of applicability and limitation in the application of each method are described in each relevant paper. Possible changes resulting from changes in context and setting are also described in the articles, as suggested by Trochim and Donnelly (2001).

3.3.3 Communicable

Communicability is assured by describing the research's background and aim and explaining research questions and the methods used for answering them.

3.3.4 Conforming

Conformability ensures that the researcher is not biased with personal values or theoretical inclinations to sway research and its findings unduly (Bryman, 2016). Strengths and weaknesses of studies are discussed to find any personal biases knowing the study being conducted and helping to correct them.

4 RESULTS AND DISCUSSION

An overview of the contribution of this thesis is shown in *Figure 5*. Research aims, papers, and results are also structured here.

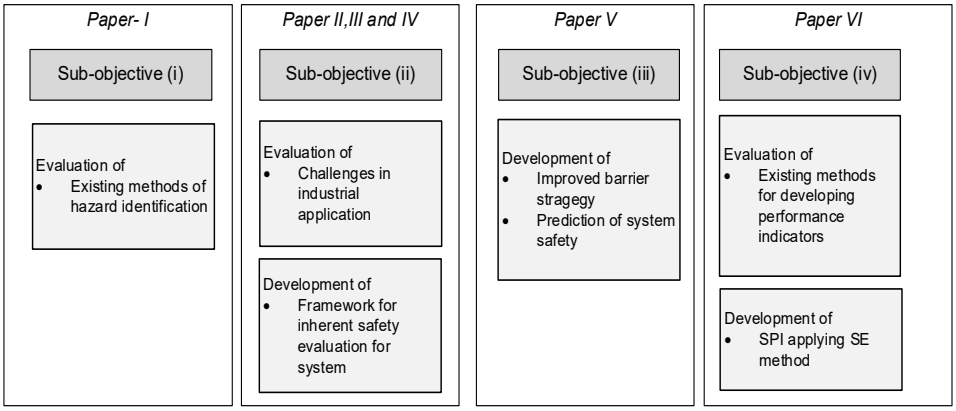


Figure 5: Structures of research sub-objectives, papers, and outputs for achieving the primary objective

The main contributions of the thesis are:

- Paper I: Improved hazard identification using SE method, application of the technique on an actual case
- Paper II: Identification of challenges of the practical application of existing inherent safety approaches
- Paper III Develop a concept of achieving inherent safety using inherent risk factors
- Paper IV: Development of inherent system safety index to choose inherently safer design between alternatives
- Paper V: An extended FRAM method to check the adequacy of safety barriers and to assess the safety of a socio-technical system
- Paper VI: Improved method of SPI development using SE method, application of the technique on a real case

4.1 CONTRIBUTIONS

This Ph.D. thesis conducts research on risk management methods that the industry can use to analyze potentially hazardous activities. This thesis focuses on four critical areas of risk management: comprehensive hazard identification, inherent safety assessment, functional safety assessment, and safety monitoring (*Figure 6*). Design improvement of the system is crucial for any facility. Comprehensive hazard identification advises on corrective action on management and organizational issues. The related methods can be used in the conceptual, preliminary, and detailed design stages. Process safety during the design phase allows for eliminating, substituting, or engineering out of hazards up-front rather than changing after the installation or after it is completed. Incorporating process safety into the design phase can also aid in deciding the proper location of vessels, storage tanks, and equipment to avoid additional facility siting hazards and better understand chemical storage volumes. With limited time and other resources, one can recognize and mitigate potential safety hazards early in a process life cycle.

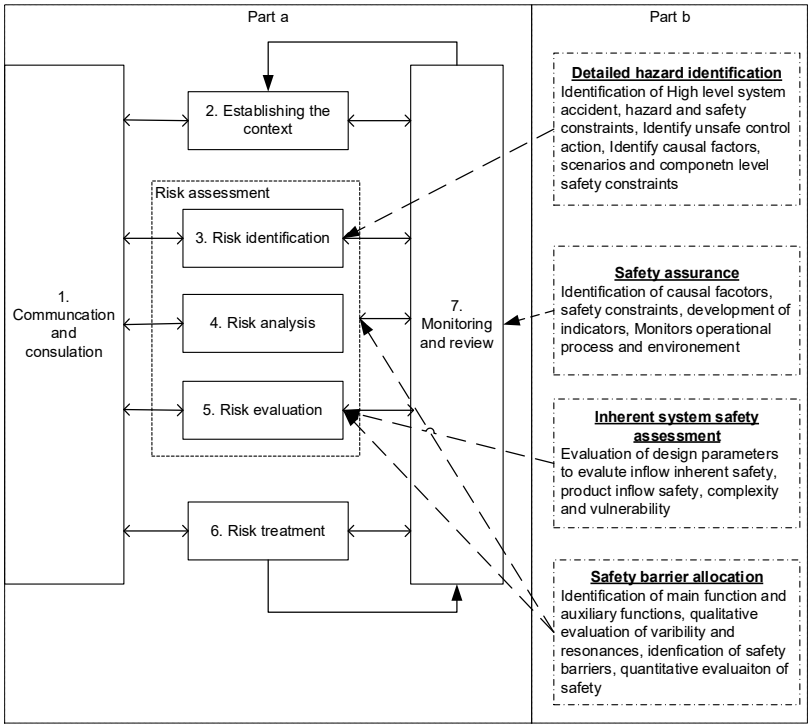


Figure 6: a) risk management of systems according to ISO 31000; b) risk management issues covered in the thesis

Inherent safety assessment and safety barrier management focus on setting up a sound system design. While in the operational stage, system monitoring is performed by assessing detailed safety performance. Implementing effective safety management will help to ensure that the organization's safety efforts target the areas where safety benefits will be most significant and, therefore, more effective. Organizations that only follow minimum standards set by regulatory agencies may not be an excellent example to proactively identify and mitigate safety hazards, especially to maintain a good safety culture. During the operational phase, safety performance is checked to ensure safety. For monitoring safety, a system-based performance indicator is advised. Based on the monitoring, safety awareness, e.g., safety training, education, regulatory compliance, inspection, or maintenance, can be recommended, and plans can be set accordingly.

The work can be considered preliminary with the considerable prospect of applying a system perspective in safety and risk management. Many methods can be involved in the overall safety and risk management process. However, the methods discussed in this research are limited to those mentioned earlier only. Other assessment methods were out of the scope of the study.

4.1.1 Hazard identification of system using SE approach

Research Sub-objective (i) identifies and evaluates existing hazard identification models and develops a SE-based method. Paper I dealt with two hazard identification techniques, HAZOP and STPA. A case study was executed with HAZOP (*Figure 8*) and STPA, evaluated and compared in the paper. An LNG ship-to-ship transfer process was chosen to investigate the feasibility of applying STPA, which requires human intervention to a significant extent, a characteristic of a socio-technical system. The reason for selecting STPA is that it provides a systematic view and focuses on the interaction and safety constraints between system components (Leveson, 2011).

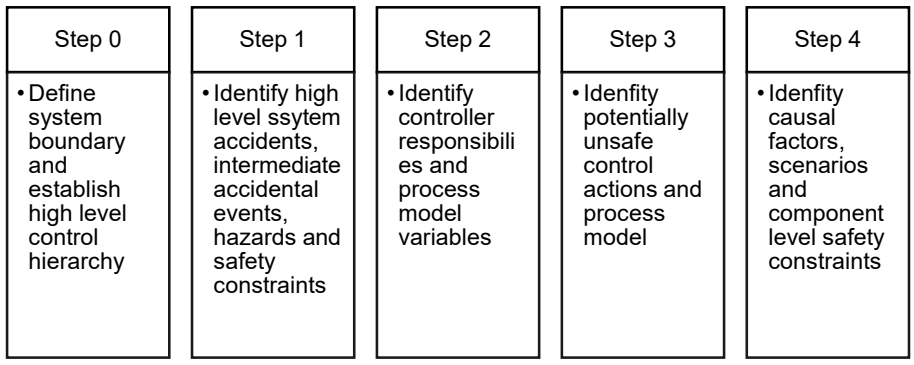


Figure 7: Workflow of STPA hazard identification method

Hazard identification in STPA started with defining the system boundaries and establishing a high-level control hierarchy (*Figure 9*). The control hierarchy diagram describes each controller's responsibilities, system behavior, and feedback mechanisms between responsible entities in the system. A control hierarchy diagram can visualize the controller, actuator, and actual procedure interactions. It identifies system behaviors and interactions to provide an in-depth method for spotting possible hazardous control actions. It depicts the paths to insufficient system control leading to a disastrous situation.

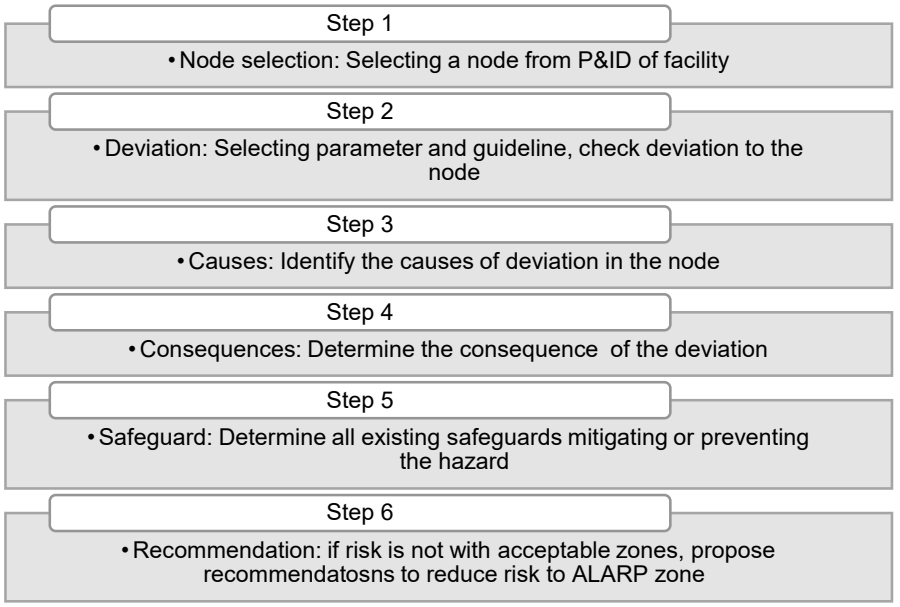


Figure 8: HAZOP methodology (IEC, 2001)

After establishing a control hierarchy diagram, possible system-level hazards and accidents were identified (Figure 7). A hazard in STPA is a system state or a combination of conditions that result in an accident when combined with a set of worst-case operational and environmental conditions. Safety constraints were identified next to avoid high-level hazards and accidents. Safety constraints are the criteria that must be enforced on the system's behavior to know safety. If the system is unable to control the hazards, accidents will occur. The hazard arises if any controllers fail to work as designed or as they should. The next stage was determining the necessary control actions to keep safety limitations. System-level safety constraints can be derived directly from the high-level hazards to prevent accidents. From the high-level safety constraints, process model variables were determined. Process model variables are those parameters that need controller actions to keep the system operating safely.

Accidents in complex systems occur due to dangerous or insufficient control activities performed by automated or human controllers (Leveson, 2004). Incorrect or absent feedback and miscommunication among several controllers may result in

harmful control behaviors. Scenarios can be developed to improve understanding of why and how hazardous control actions occur and the associated cause elements. STPA investigates the critical functions of each entity in the control loop and the prerequisites for effective safety system behavior. Goals and related system performance can be redefined, and alternatives for analysis can be developed. This method highlights the significance of the process model in ensuring appropriate control. A hierarchical control model depicts system behavior in relationships that indicate the system's structure. Before building the comprehensive process and instrumentation diagram (P&ID)., one might work with STPA with the help of a main process flow diagram (PFD).

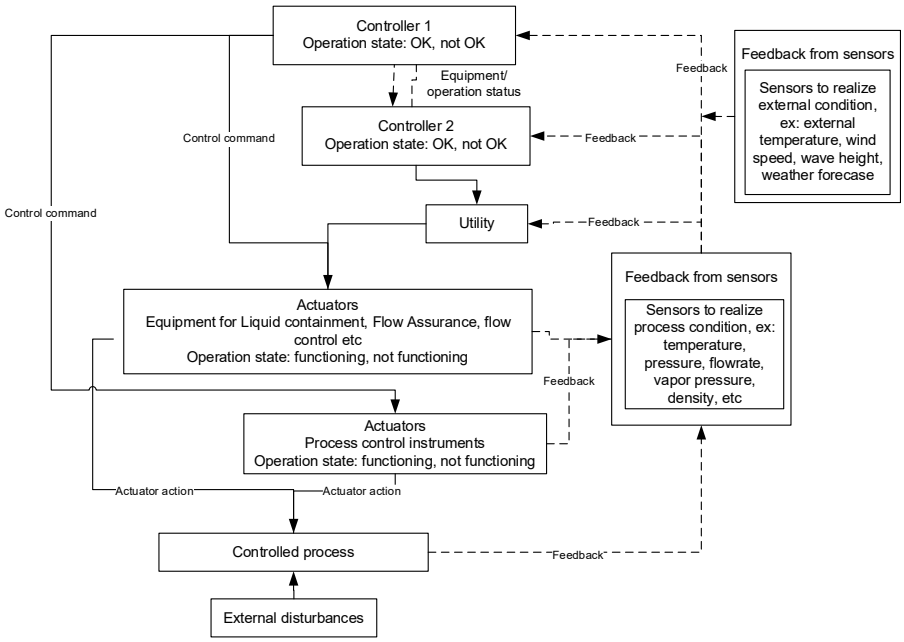


Figure 9: Control hierarchy diagram of a process system in STPA

STPA is a systematic hazard analysis technique that gives systematic guidance and suggestions for safety requirements, according to the comparison results. The fundamental difficulty in STPA is establishing the control structure. On the other hand, developing the control structure is advantageous because it provides extra insight into how the system functions, particularly at the higher level of the hierarchy. STPA can study large systems' behavior with highly automated features and multiple component interactions. It can lower non-identification risks and create different control structure diagrams ranging from high to detailed.

The investigation revealed that, when it came to identifying the technical flaws of the component, the hazard lists for HAZOP and STPA were identical. HAZOP is an effective method for identifying and evaluating component-related hazards connected with processes used in the petroleum and chemical industries. It is considered suitable for identifying hazards arising from single, independent contingencies. It can identify any deviation in the system quickly.

However, in STPA, success depends on correctly identifying high-level unintentional events. Low-level dangers that do not fall into the category of any high-level unintended incidents or hazardous control activities can remain excluded from the scope of the study. In STPA, using the control hierarchy diagram, the effects of external events can be identified conclusively and systematically. HAZOP uses a deductive or downward technique to determine what will happen due to deviations, such as top events and deviations.

HAZOP is less efficient than STPA in treating software errors because identifying software errors requires a good understanding of software behavior, interactions, and effects on other systems, which is difficult in the case of complicated software. Resource requirement was seen as the same for both cases. Experts from all disciplines must participate face to face and check the deviation or high and low-level hazards. Feedback from all discipline experts should be considered to find the deviation or safety constraints, e.g., electrical, automation, instrumentation, software, and process. As STPA is a new method, the user may not be confident using it, even if it is superior. However, users may gain confidence in using STPA from its level of detail.

HAZOP has become widely recognized for systems analysis due to its straightforward approach (Hoepffner, 1989). STPA, on the other hand, is a new method that has yet to be adopted widely, particularly in the process industry. Execution may be difficult for industry professionals. It can be difficult to identify causal elements and conduct the steps in the procedure. This disadvantage of STPA may indicate that it should be utilized for more confined areas of the system, which are difficult to examine with HAZOP.

The case study of the investigation demonstrates that STPA can address a broader range of organizational mistakes. Compared to STPA, identifying organizational flaws in a HAZOP is more complicated because HAZOP was created to discover system deviations in the process sector, not variances in human behavior or organization. STPA illustrates the entire system and its interactions with other components and their impacts on the system using a hierarchical control diagram. Organizational defects and requirements can be included since it uses a systematic method to detect safety constraints. The control hierarchy and system used in the case study only cover a small system component, the ship-to-ship LNG transfer procedure, and do not address many organizational elements. More organizational flaws could have been discovered for an expanded structure.

STPA, in general, can go into greater depth in determining the causes of failures by its control-hierarchy diagram and process model. Application of its four keys like

‘not provided causes hazard, ‘provided causes hazard,’ ‘too soon or too late causes hazards, and ‘applied too long or too short causes hazard’ increases confidence that all potential threats are identified. Users can dig into the details of each issue of system requirements by refining each accident and safety constraint at a lower level. However, setting the study's boundaries, determining the required number of variables to be investigated, the necessary control actions for each safety constraint, and the role of controllers for each control action needed in STPA are complex tasks in process industry applications.

The most notable strength of STPA is its well-organized control diagram. However, the effectiveness of STPA is dependent on the proper development of a control hierarchy diagram. A chaotic control hierarchy diagram can result in incomplete and entirely useless analysis. In STPA, situations and causal factors are straightforward, utilizing the human controller model as a starting point instead of a typical human factor model. Before finalizing the system design, it can address difficulties linked to human-automation interaction. The human operator's involvement in system operations can be examined, and the design can be adjusted accordingly. One advantage of having a human in the control loop is the capacity to modify or develop new processes.
The case study under consideration was a simple system. A more complicated system may produce drastically different results. STPA is more suited for use in a complex system because it seeks out hazards in a systematic manner. The difficulty of STPA would be dealing with several variables and controllers, the number of state variables, the number of variables, and, most importantly, setting the system limit (Rodriguez and Diaz, 2016). Moreover, the time required to conduct STPA may become exceedingly long for complex systems compared to HAZOP. The additional time is reasonable because STPA provides a complete study and requires less time to modify future plants. Overall, adopting STPA is that the analysis is quite systematic and appropriate for use in a socio-technical system. The mitigation approach can be efficiently designed and evaluated using scenario control algorithms. STPA can capture dynamic system behavior. The root situation can communicate the necessity for further mitigation strategies at the board level.

4.1.2 Development of a framework for an assessment of the inherent safety of a system

Research Sub-objective (ii) evaluated the challenges of industry application of inherent safety and developed a framework for inherent safety evaluation of the system. Paper II, Paper III, and Paper IV addressed this objective. Paper II reviews inherent safety assessment techniques, explains industry application challenges and suggests probable future methods. Challenges in applying inherent safety in practice are related to difficulties in implementation, interpretation of the results, lack of consideration of overall scope, and dimensionality problems. Details are described

in Paper II. The paper's findings inspired further research in this direction. Often overall, system thinking is missing in the earlier methods.

Paper III presents a novel concept of achieving inherent safety by considering a system's inherent hazards and risk factors. Hazard is the existence of factors that can cause harm to people, the environment, or assets. Hazard factors can be properties, circumstances, or causes that have the potential to cause damage. Hazard factors are classified into two types: triggering hazards and impacting hazards. Triggering hazard factors are those that can directly create a hazardous event. The presence of motion indicates the presence of kinetic energy, which can result in a hazardous event. As a result, motion is a triggering intrinsic hazard factor. Impacting hazard factors do not directly contribute to creating a hazardous event but indirectly impacts the intensity or probability of a hazardous occurrence.

An inherent risk factor is the quantitative expression of the two categories of hazard factors, triggering and influencing intrinsic hazards. Triggering inherent risk factors contributes to the creation of a hazardous event. In contrast, impacting inherent risk factors does not contribute to creating a hazardous event directly but may affect the system's inherent hazard factors or risk level, thus changing the probability or severity of the hazardous event. The conceptualization of inherent risk factors assumes that the risk level (in terms of a quantitative measure) can be controlled by changing/ managing/ controlling the inherent risk factors (*Figure 10*). Two main strategies should be followed to achieve IS of a system: i) Reduction of the severity of triggering inherent risk factors, ii) Modification of impacting inherent risk factors.

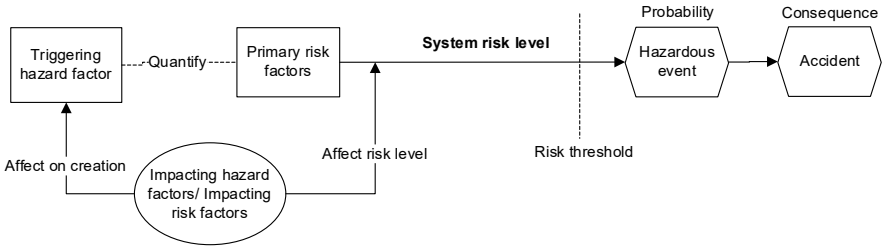


Figure 10: Relationship between inherent hazard factors, risk factors and hazardous events

The severity of triggering inherent risk factors can be achieved by proper selection of material, modification of material, equipment, or reaction, minimization of hazardous material or equipment, the transformation of material or equipment, recycling of material to reduce hazardous material usage and energy consumption, relocation of equipment, rearrangement of facility layout, comprehension. Modification of impacting factors can be achieved by modifying geometry or shape.

Previously, achievement of inherent safety was described by selecting various principles, e.g., intensification/minimization, substitution, attenuation, and

simplification as proposed by (Kletz, 1985) and other principles like error tolerance principles, making incorrect assembly impossible, making status clear, easing control, integrity, software, reliability, limitation of effects (Heikkilä, 1999). However, these principles are challenging to apply systematically in a practical case. There may thus be uncertainty in selecting and applying appropriate inherent safety perspectives. The principle "limitation of effects" may create confusion as passive and active measures are also used to limit consequences.

So, it is difficult to see the risks carefully in practical cases when choosing between alternatives. Systematic identification of inherent risk factors can help analysts to achieve inherent safety by modifying the risk factors or taking actions in such a way as to reduce the severity of those risk factors. Relevant knowledge about inherent hazards and risk factors can be gained from similar industries' accident databases. Considering the cost, considering system hazards will be most beneficial at the design stage when the opportunity to modify and improve the design has the highest scope.

Paper IV presents a method to determine inherent safety in a specific system. The framework consists of four steps. The first step determines inherent safety characteristics and related parameters (*Figure* 11). The second step determined the characteristics of a perfect, inherently safer system and corresponding numerical or qualitative values (*Figure 12*). In the third step, the deviation of the real system from the perfect system is determined based on the deviations of the parameters defined in the earlier step. The Inherent safety index is determined based on their deviation in the last step.

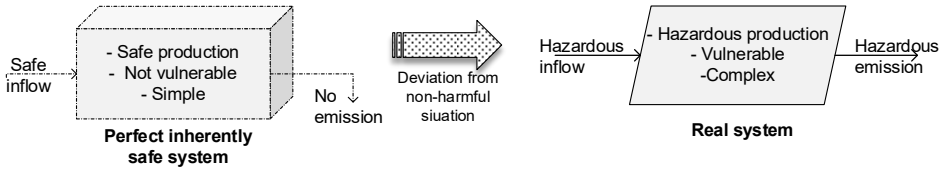


Figure 11: A perfect, inherently safe and a real system

Figure 12: Framework of ISSI calculation

The proposed method in Paper IV considers health, safety, and environmental perspectives to evaluate the inherent safety of a chemical process route. Inherent safety techniques frequently restrict examining only a subset of factors. Various essential elements can be focused on based on a system's kind, nature, or location when considering inherent safety parameters produced from inherent safety characteristics. Unlike most existing methods, the suggested method examines

materials as streams rather than individual materials (Heikkilä, 1999). If just the most hazardous material is considered in the analysis, the option to improve the design by substituting hazardous materials becomes limited.

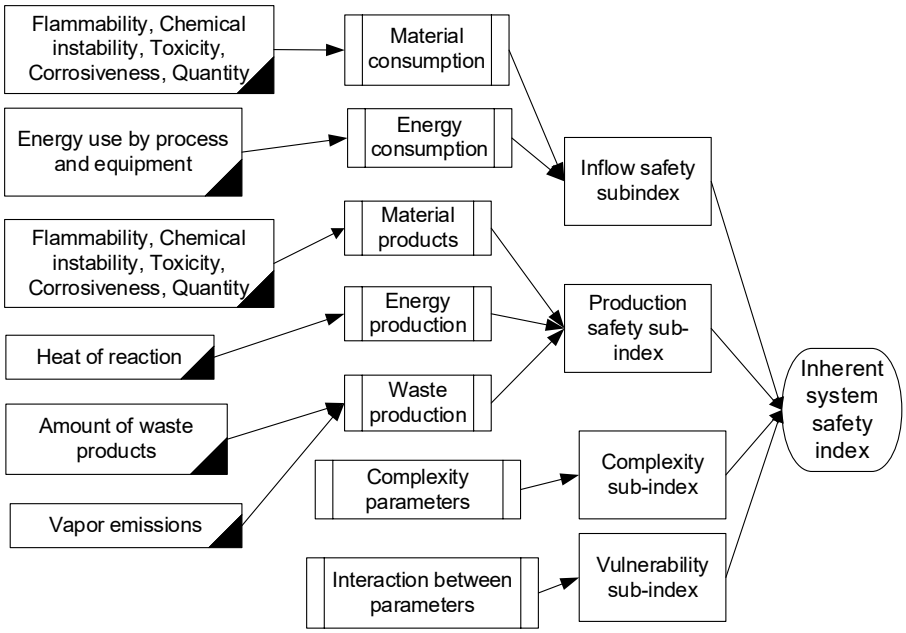


Figure 13: Calculation of inherent system safety index

The ISSI consists of four sub-indices: inflow safety, production safety, complexity, and vulnerability. Inflow safety in a chemical process relates to the safety of materials taken by the system each day or hour and storage inventory. The inflow safety sub-index consists of deviations due to the presence of hazardous material in the inlet, the process's energy consumption, and the energy consumption of the equipment. Five crucial material properties were considered to calculate deviation due to inlet materials in a chemical process. They were flammability, chemical instability, corrosiveness, toxicity, and quantity, as these attributes can provide a reasonably good indication of material safety (NFPA, 2017).

High energy consumption will result in high demand for electricity or other energy sources. Because high energy control is complicated and dangerous (Klugmann-Radziemska, 2014), low energy consumption is considered an inherent safety feature of the method. The deviation of each parameter is determined from tables of deviations. A minimum deviation is assigned as zero, and the highest deviation is set as ten. Various deviation scores were assigned based on their potential for harm. For example, zero is assigned to non-flammable materials when calculating a

flammability deviation score. Ten is awarded to highly flammable elements with flashpoints lower than 0ºC. Deviation due to equipment energy consumption is calculated by energy consumption by individual equipment, the efficiency of individual equipment, and the total number of equipment. The energy consumption of a process is calculated by the energy balance equation of a steady-state process.

The production safety sub-index consists of deviations due to material properties produced in the process, deviations due to the heat of reaction, deviations due to emissions, and deviations due to the amount of waste material in the process. Steams or vapors emitted from the process were considered emissions here. To find waste material's deviation, the number of chemicals in effluent streams and the score of those chemicals were considered. Scores of chemicals were determined based on their waste code which considers ignitability, corrosiveness, reactivity, and material toxicity (BAKER et al., 1992, Rosenfeld and Feng, 2011). The amount of flammable vapor produced immediately from a liquid at a temperature above its atmospheric boiling point can be calculated considering the mass of flammable vapor released, the mass of liquid, specific heat of the liquid, liquid temperature, and the heat of vaporization at the boiling point of a liquid (King, 2016).

Complexity index is determined by the parameters that affect the process's control requirements. The control of operators and maintenance personnel becomes more challenging as process configuration becomes complex. ISSI uses the method described by Song et al. (2018) to rank complexity with a few modifications. Process complexity is considered based on fourteen parameters. The parameters were the number of input streams, number of output streams, number of condition changes, number of mixing steps, number of changes in the state of process materials, number of flashing liquids, number of flashing inventories at ambient, number of time-critical operations, number of sequence-critical operations, number of critical changes of operations, equipment ranking, number of recycling of the process, number of stages, and number of unstable intermediates.

The process flow diagram and description of each route can collect information such as the number of input and output streams, the number of changes, mixing steps, and state changes. Equipment is classified based on its hazard rating without regard for its failure rate. Furnaces and flares were deemed more dangerous than reactors since they are the most common ignition sources for leaks (Instone, 1989, Planas-Cuchi et al., 1997). The safest equipment is the equipment handling nontoxic and non-flammable material. Reactor pumps above autoignition are more hazardous than process drums.

The vulnerability index is generated by taking into account the vulnerability of the processing system as a result of specific processes, parameter interaction, or excessive values of any specific parameters (Lawrence, 1996). For special procedures requiring unique control characteristics, various penalty factors were imposed.

Hydro-generation, hydrolysis, isomerization, and alkylation, for example, necessitate specific handling (Heinemann, 1979). The interaction of various

parameters raises the risk level of a system. Because of the interaction of numerous characteristics, the aggregate risk of a system may increase, and accidents occur with greater severity in these circumstances (Lawrence, 1996). Penalty factors were assigned based on potential interactions among various system parameters. For example, the internal properties of the material are critical in raising risk due to flammability, toxicity, or explosion qualities. External properties such as quantity play a critical function in the system when these properties are present. Regarding risk increment, process parameters follow a similar pattern when the pressure rises, the temperature rises, and the flow rate falls.

Chemical interactions also introduce additional risks in the plant-based reaction or intermediate products. Penalties for chemical interactions were assigned based on the US Environmental Protection Agency (EPA) matrix (Hatayama, 1980) and hazard classification of chemical interaction (Heikkilä, 1999). The formation of highly toxic or flammable gas gets the highest penalty as it may cause the most hazardous accident, fires, and explosions. Highly flammable or highly toxic material needs extra precautions for safety (Kletz, 1995, Lawrence, 1996). Additional scores were assigned to consider these risk level changes, termed penalties.

ISSI is calculated finally by summing above mentioned four subindices. In the case study of Paper IV, ISSI is calculated for various routes of the production process of Methyl Methacrylate (MMA). The inflow system safety index, production safety system, vulnerability, and complexity indices were calculated for each route. The ranking of routes is done based on their ISSI index value. The route with the lowest ISSI index value is inherently the safest and highest. For MMA production, the ACH (Acetone Cyanohydrin) route was found most inherently unsafe, which was logical as it has the most substantial number of stages, equipment, and streams, increasing its complexity and vulnerability. The ACH route was most hazardous considering its complexity and vulnerability, as it has many unstable intermediates and steps. C2-PA (Ethylene via Propionaldehyde) has the highest hazardous inflow to the route. TBA route was found inherently safest; it has lower steps, lower hazardous inflow, and lower complexity and vulnerability.

In the proposed method of Paper IV, various deviation scores were assigned to parameters considering their hazard level to remove the dimensionality problem. Adding parameters of different dimensions like temperature (◦C), pressure (atm), inventory (t), toxicity (ppm), and comparing the summed value is unacceptable from the engineering point of view. The terms need to be dimensionless, or the score parameters based on their hazard rating. The reflection of vulnerability ensures consideration of interactions between various risk factors in the model. Various penalties are assigned for temperature above autoignition, boiling point, or flashpoint.

The unjustified measurement of the many parameters is compensated for by imposing several penalties, such as high pressure, high temperature, or high toxicity. Penalties were set for the existence of high temperatures and special vulnerable equipment. The subindices can be addressed individually if extra attention is

required in a specific segment. For example, the production sub-index can be calculated for many alternative designs to determine the inherent safety standpoint of a smaller portion of a facility, such as a reactor.

4.1.3 Allocation of system safety barriers using the SE approach

In Paper V, an extended FRAM method is used to check the adequacy of safety barriers and assess the system's safety based on the performance of safety barriers. The method is applied for a practical industry case, LNG ship-to-ship transfer. Safety barrier management is vital in process safety and risk management to reduce risk and keep risk factors in control. With the development of modern automated systems, new risks have evolved due to the complexity and interaction of various components. It has become difficult to capture these effects by using traditional methods. In conventional techniques, accidents are considered a linear chain of consequences of failure of existing barriers. The traditional barrier approach assumes constant barrier performance, and risks are measured based on static values.

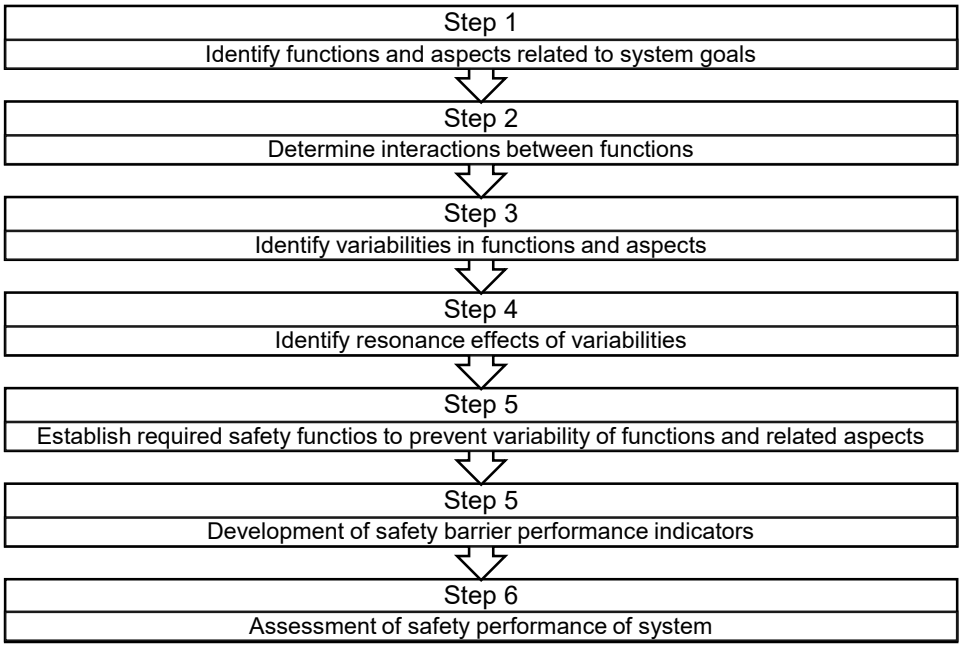


Figure 14: Workflow of extended FRAM

In FRAM, the system is decomposed into system functions. It considers input, output function, time, control, precondition, and resource. FRAM can capture the interaction between system elements. The method starts with identifying the main and auxiliary functions required to be executed to achieve the system goal (*Figure 14*). The main functions are related to plant goals. Auxiliary functions are additional functions related to main functions or required to execute the main function. After

identifying main and auxiliary functions, related aspects are identified. The FRAM model determines the coupling between various aspects and functions and presents graphically (*Figure 15*). In the next step, the variability of functions and aspects is identified. In the work of Paper V, four kinds of performances were considered for each aspect: precise, omitted, imprecise, too late/stopped in the middle.

When a function is executed in the specified time and precision, it is said to be 'precise.' If a function is not fulfilled or an aspect is absent, it is referred to as 'omitted.' An imprecise function is conducted with unacceptable precision. A function can be tracked independently if it is too late or stopped in the midst. A function's variability is strongly related to its aspects or aspects of other functions. Any modification in these aspects' performance will influence their output function and the system's purpose. The performance variability of the system is reflected in the performance of upstream functions. When the variability of many functions resonates, the outcome of upstream functions fluctuates unexpectedly. Accidents do not evolve from non-execution or performance deviation of one function but the resonance effect of performance deviation of multiple aspects in a system.

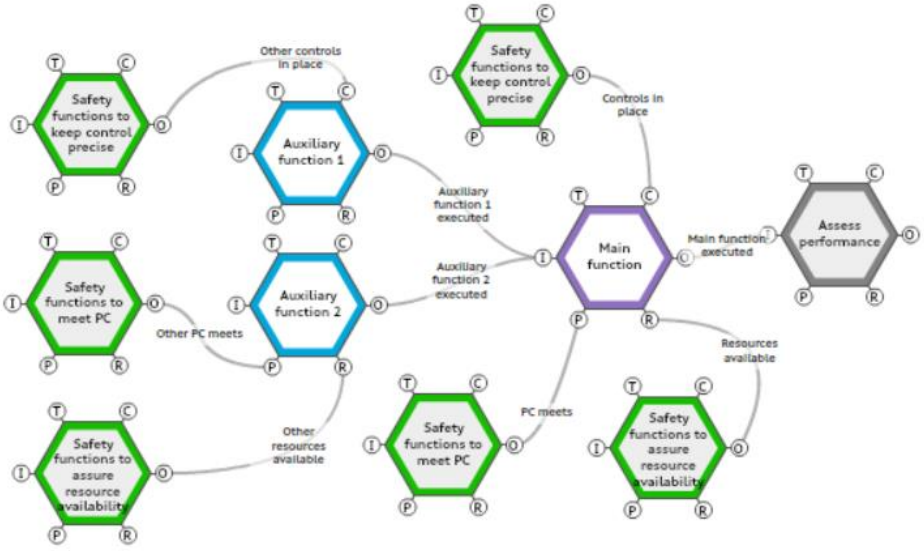


Figure 15: Execution and main function, auxiliary functions, safety functions, and their interactions in FRAM diagram

Later steps of the technique covered causal components of variability or resonant effects of variability. The necessary safety functions were then identified to prevent variations in the performance of aspects and functions. There are three sorts of safety functions: (i) safety functions that nullify the reason for the abnormal state of functions that resonate from downstream functions and aspects, (ii) safety functions

that mitigate the abnormal state that affects upstream functions, and (iii) safety functions that nullify the reason for the abnormal state caused by an external effect.

There can be various safety functions to prevent a single variability. These are termed barriers in general terms. All the possible safety functions should be considered to achieve the redundancy of barriers in the system. In FRAM, barriers are conceptualized as safety functions and presented in the graphical model.

Safety barriers' performance indicators were developed based on required safety functions determined in the earlier step. A safety performance assessment method is presented later, assuming the system consists of multiple levels. The performance of the target function depends on the contribution of various aspects from different levels. The level distinction is made based on the sequence of execution. Performance variability of a function or aspect at one level will affect a related function or aspect at the next level. Due to interaction or coupling between aspects at various levels, resonance effects can evolve. Two factors were considered for the quantitative safety assessment: aspect weight and variability. Three weight factors were considered: 'low,' 'moderate,' and 'high.'

If a function is related to the main function, so the performance of the function will affect the system goal, then the weight of the function is 'high.' If a function is not related to the main function or any auxiliary function, the performance of the function will not affect the system goal; instead, it will affect the performance of other functions, then the weight of the function is 'moderate. If a function is not related to the main function or any auxiliary function, to any safety function, but there are also other safety functions to execute the required function, or the aspect, the performance variability of the function will not affect the system goal significantly. The weight of the function is 'low.'

The ideal state of each aspect is used to calculate a variability score. When each aspect is in its ideal state, variability is zero. If the variability is zero, the output will be precise in quality and time. A zero to four variability table is constructed to determine the overall output score, with four being the most and zero representing the most negligible variability. A maximum variability of four can indicate no output from the output function, resources are entirely lacking, a pre-condition is not met, or control is not present. Each variability is related to the variability of its downstream aspect situated at the earlier level. A calculated score represents the prediction of the variability of a specific function at a particular point in time. The correlation between aspects is determined by building a correlation table to consider overlapping or resonance effects of variability of aspects. Variability scores were revised considering the correlation between factors.

The case study used FRAM-STPA, the bowtie approach, and a Bayesian network (*Table 2*). Both FRAM and FRAM-STPA can provide a quick method for determining the sufficiency of safety barriers. In the FRAM-STPA method, STPA keywords were used in the FRAM method to find variability causes in the plant. The first few steps of this method were the same as the FRAM method. STPA helps in identifying the deficiencies in establishing a safety constraint. Safety barriers are

placed in the system to ensure proper causal constraints. Each barrier executes individual functions. Upon failure of those barriers/in the absence of the functions related to those barriers, constraints will not be fulfilled. So, the execution of the related function will not be executed.

Table 2: Comparison among Extended FRAM, FRAM-STPA, Bayesian network, and Bowtie model:

Evaluation aspects	**Extended FRAM**	**FRAM-STPA**	**Bayesian network**	**Bowtie**
Complexity	Medium	--	Medium-high	Medium
Ability to represent a complex relationship	High	Medium	High	Low-medium
Competence requirements	High	Medium-high	Medium-high	Medium
Computational procedure	Multilevel mathematical	--	Probabilistic	--
Acquaintance of procedure	Low (used only in academia)	Low (used only in academia)	High (Widely known and used)	High (Widely known and used)
Failure identification	Resonance of variability	Violation of safety constraints	Effecting variables	Top events and threats
Barrier allocations	Functions to resist variability	Control actions to establish safety constraints	Modifying variables to reduce the probability of an outcome	Preventive barriers to eliminate/control threats, Mitigative barriers to reduce consequences
Observation of delegation of authority	By identifying resources and controlling for each function	By identifying sensors, controllers, and actuators in-process model	Various colors in the graphical model	The multiple colors in the graphical model

The case study shows that both FRAM and FRAM-STPA suggest an almost similar number of barrier elements required for the system. FRAM and FRAM-STPA can be used for hazard identification and mitigation procedures and as an alternative to HAZOP and STPA. Comparing with HAZOP and STPA, it is seen that both FRAM and FRAM-STPA can give a better overview of a scenario of system mishaps and resisting barriers or functions can be better planned accordingly.

A significant advantage of the bowtie model is that it is an easy and time-conserving model to identify barriers. Specially bowtie model can emphasize the prediction of consequence effect, and barriers can be considered accordingly. On the contrary, a significant disadvantage is that it does not consider any coupling or interaction between threats or multiple barrier failure. A comparison of the bowtie with FRAM shows that, in addition to the limitation of consideration of coupling, it has several other limitations over FRAM. For each function execution, resources and controllers are identified in FRAM. So that it is clear which authority, process, or equipment must be ensured for function execution. Also, FRAM gives dynamic analysis to consider time constraints, which is a significant limitation in a bowtie.

A Bayesian network can find coupling or interaction of multiple barriers in the system. Change of status with time can also be captured (Yeo et al., 2016). However, one weakness of the Bayesian model is that job allocation or task authority is not immediately observable. When various components and complicated interactions are considered, each barrier's essential resources or controls must be identified in a sophisticated graphical model. More resources and work hours will be needed for this sophisticated structure. FRAM produces more specific details than Bayesian by considering the functional resonance process. Performance variables of the entire system can be understood in much detail with its graphical model. FRAM can give more comprehensive results and capture qualitative, quantitative, and dynamic variability characteristics.

The qualitative characteristics of variability can be captured both for functional output and for outcomes of the entire system. Capturing qualitative variability features can assist analysts in identifying sources of variability that influence the output of downstream processes and, potentially, the overall system outcome. Output variability of a function can be expressed numerically on a scale of zero to four. Apart from the reflection of the performance of related aspects, there can be many other uncertainties in the system, which may affect the performance of the output function. Quantitative analysis can compare the system performance at two different times or compare two similar systems. If the quantitative number ranking indicates that the system is not performing well, efforts should enhance system performance.

The model can capture time variation for a specific function and system. The execution time of the function is variable for various cases. The time variability may affect upstream functions and may even influence the outcome of the entire system. Understanding the time variations in the functions' executions and their effect on the system can help improve the system's quality.

A disadvantage of FRAM is that it is time-consuming, which was also proved in the investigation of Pezeshki (2020). In the future, when studying a complex socio-technical system, such as installing an LNG network in a residential area where a minor deviation can have a significant impact on the company's reputation and economy, this type of analysis will assist analysts in taking the necessary steps to ensure safety and reduce system performance deviation. More case studies with additional industrial cases could be done in the future.

4.1.4 Development of safety performance indicators using the SE approach

Sub-objective (iv) evaluates the existing methods for developing safety performance indicators (SPIs) and the development of SPIs applying the SE method. Paper VI addresses this objective. Various guidelines like UK HSE and the OECD describe procedures for establishing SPIs (Jennings and Schulberg, 2007, OECD, 2003, HSE, 2006). Paper VI describes a SE-based strategy for developing safety indicators. Three main tasks were performed in this work. The first task was to formulate a method for developing SE-based safety indicators. The second step was to apply it to a case study, and the third was to compare the approach to the approaches proposed by OECD and CCPS already established in the industry. The paper used the STAMP accident model.

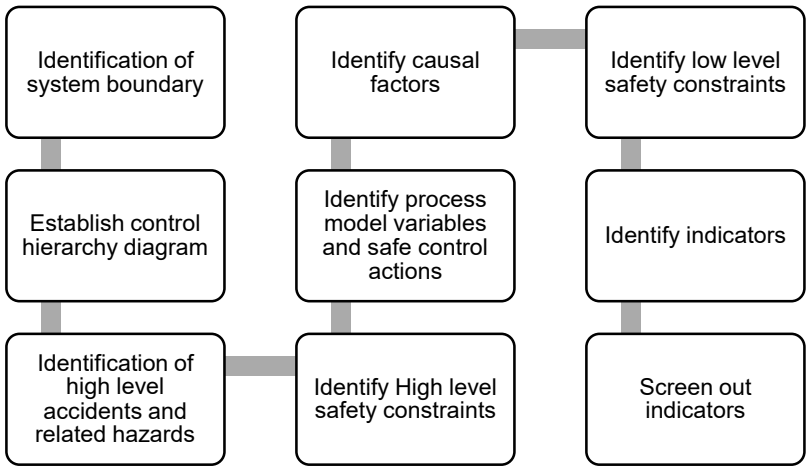


Figure 16: Development of safety performance indicator program by STAMP

Figure 16 shows a process flow of safety performance indicator development by STAMP. Establishing the scope of the safety indicator development program is the first stage in the indicator development model. A description of the system, essential hazards, related safety barriers, and safe operational limits should all be included in the scope. The system's boundary is established based on the established scope. The next step is to model the system as a control hierarchy structure. This process entails gathering and compiling information and data on the system, site, and associated

activities that are being investigated. The system requirements and interactions were used to construct a control hierarchy structure. Each entity performing a given action is specified to build the structure.

After constructing a control hierarchy diagram, high-level hazards, high-level safety constraints, and hazardous control actions were identified in the same manner as typical STPA. After identifying potentially hazardous control actions, the following step is to figure out how these can happen or how hazardous conditions can develop that can lead to an unstable system state or accident. Potential safety indications were developed based on the safety constraints identified in the previous step. The performance of the related subsystems is reflected in the indicators. For each constraint, one or more indicators can be identified. There can be two indicators: indicators reflecting technical issues and human-organizational issues.

The proposed method uses the LNG ship-to-ship transfer process as a case study without specifying precise process parameters. At the conceptual design stage, developed indicators can assess safety. STPA can determine safety requirements and restrictions during the concept phase. The analysis can address potential causal situations of accidents and check the proficiency of accident prevention techniques such as redundancy, barriers, human intervention, operational procedures, checklists, and training. Scenarios can be used to generate new requirements such as mitigation or new design decisions. STAMP has the advantage of making it adaptable to plant or system component changes. The associated hazards, safety constraints, and controller actions must be identified for modification, and performance indicators must be developed accordingly.

An extensive list of indicators was created during the initial development of indicators. Continuous monitoring of many indicators takes time and money. Indicators must be screened based on the organization's mission, expected performance, and desired safety goals. Fifty-five indicators were identified from previously determined safety constraints. Indicators were screened out, and fourteen indicators were finally chosen for monitoring. The screening was done based on the authors' recommendations from practical industry experiences. Indicators covered several topics, i.e., mechanical integrity, documentation and procedure, human resource management, inspection, maintenance, audit, risk assessment, training, and competence work permit system. The level of reliability of critical safety equipment, percentage of shutdown/isolation system functioned desired performance standard, adequacy of documentation on emergency response action, and status of inspection in a year of safety-critical instruments are some of the developed indicators.

Established indicators were a mix of leading and trailing indicators. Indicators were leading in that they emphasized proactive action before accidents, such as insufficient inspection and maintenance checks of the shutdown system. Some indicators can be lagging; for example, no automated system problems have been recorded, and no operators have indicated inaccurate settings. A leading indicator-based system can track the control system's effectiveness, improve safety performance, and lower the probability of an accident or serious incident.

A challenge related to the SPI program is determining the indicators' thresholds. Facilities can define their threshold values based on practicality, target risk level, and additional cost to achieve the objective or authority requirements. STAMP is highly beneficial for detecting early warning signals as it may identify faults at the source, and actions can be taken swiftly. It provides early warning of deviations from the design and operating safety standards and can detect degradation in safety performance as soon as possible. Monitoring STPA's indicators are straightforward, yet, it can be resource-intensive. Indicators were plant-specific. Because it ties to unforeseen events that the organization wants to avoid, the STAMP-based strategy focuses mainly on operational indicators.

Comprehensibility is an essential quality for indicators. The relationship between the indicator and the risk factor is simple to understand, and the indicator's significance is easily visible. It offers the advantage of measuring present conditions and early warning of possible problems. Before an accident, certain clues indicate that something is wrong, while others can reveal what is wrong. The method makes it simple to track the deficiency in operation responsibility because it stems from the operator's lack of control action that can be changed into an action list.

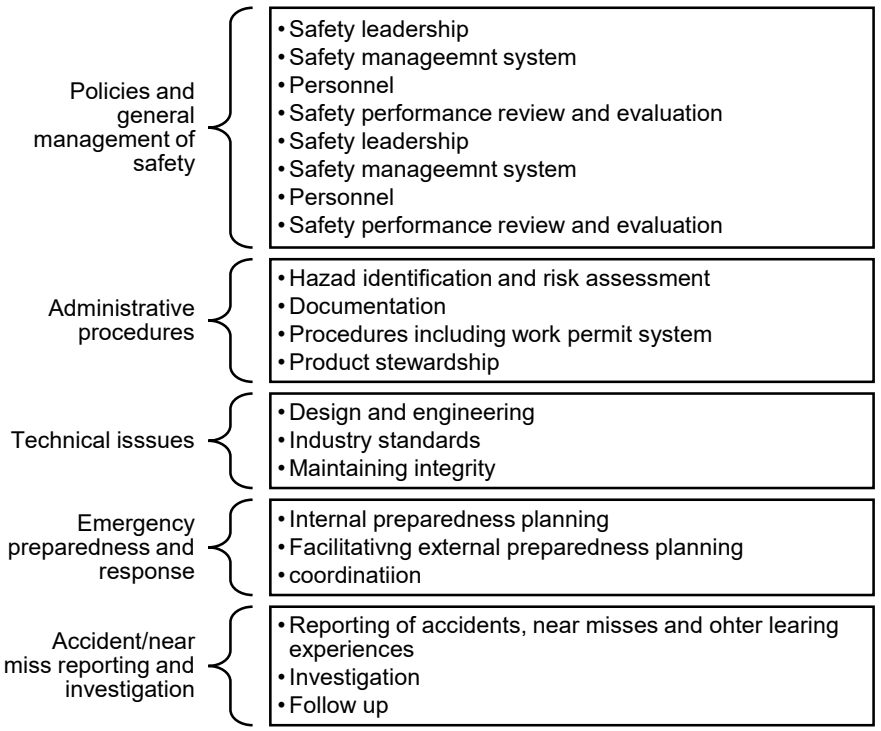


Figure 17: Issues covered in the OECD indicator development model

The OECD guidance includes predefined sets of indicators (*Figure 17*). It has many indicators, especially in hazard and employee safety management. The OECD

guidance does not specify a technique but offers suggestions for creating and applying safety performance indicators. The guidance defines two types of indicators: activity indicators and outcome indicators. The work develops six categories of outcome indicators: general safety management, administrative, technical concerns, emergency planning, and accident reporting.

Indicators based on STAMP were plant-specific, while the OECD guidance has predefined sets of indicators. It provides a comprehensive set of indications for hazard and personnel safety management. The STAMP-based strategy focuses on operational indicators since it identifies risky control actions that result in unanticipated events that the company wishes to prevent. An unexpected event's causal chain can reveal all relevant organizational issues. However, the problem with the presented case study was that the system was narrow and did not incorporate the entire organization required to run it.

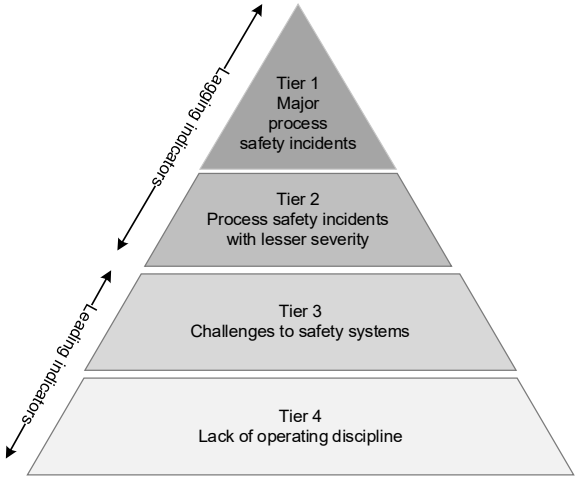


Figure 18: CCPS process safety metrics

On the other hand, CCPS's leading and lagging metrics consider tier one and tier two process safety incidents, tier three and tier four safety systems, and organizational deficiencies (*Figure 18*). Tier one process safety incidents based on process involvement, above the minimal reporting threshold, location, and acute release. Tier one incidents are defined as the unintentional or uncontrolled release of any material from a process, including non-toxic and non-flammable materials, resulting in severe consequences such as employee injury or death, evacuation, fire or explosion, and the release of toxic substances above a defined threshold (CCPS, 2007). Tier two Process Safety Events are occurrences with a lower severity than Tier one process safety incidents. A Tier two incident is an unintentional discharge of non-toxic or non-flammable substances, such as steam, hot condensate, compressed CO_2, or compressed air, with fewer consequences than a Tier one event.

CCPS establishes industry process safety measures, making it easy to compare events over the years and assess the plant's overall safety performance. Tier one process safety incidents with high consequences and tier two process safety events with lower effects are considered in the CCPS lagging indicators. Tier two lagging indications should be given special attention to early warning signals. CCPS lagging and leading indicators were developed during the present research. Lagging metrics are a set of metrics calculated retrospectively based on occurrences that reach a severity threshold as part of an industry-wide process safety indicator. Leading metrics highlight the effectiveness of the safety management system and provide an early warning of deterioration in the effectiveness of these vital safety systems, allowing remedial action to be conducted before a loss of containment event occurs.

Maintenance of mechanical integrity, action item follow-up, Operating and Maintenance Procedures, Process safety training and competency, and Fatigue risk management were some of the leading safety metrics developed. The 'mechanical integrity metric' is one way to assess how well a risk management system is performing to ensure that safety-critical plant and equipment are operational. The metric 'action item follows up' determines the number of safety important plant and equipment inspections accomplished throughout the measurement period (CCPS, 2007). This indicator determines how well the plant can quickly correct discovered flaws in process safety equipment. 'Process safety' and 'competency training' are used to assess the effectiveness of process safety culture in chemical processing companies. Compared to OECD and STAMP indicators, safety management systems derived from CCPS safety indicators provide a thorough overview of the plant with less effort and money.

According to the findings, STAMP-based modeling provides a more profound knowledge of the system. The STAMP-based indicator generation approach aids in focusing on specific issues that could lead to danger. It considered human and organizational factors and technical elements to mitigate or prevent high-level and low-level system hazards. Another benefit is that STAMP-based indicators can easily be modified or revised for any plant or system component change. OECD gives an extensive set of indicators, especially in hazard and personal safety management. It was discovered that the STAMP-based approach necessitates a significant amount of effort to enable the control hierarchy and complete the remaining procedures. However, given the variety of methods and the depth of the research, the work is worthwhile.

In terms of early warning potential, area of emphasis, amount of information on the study, ability to focus on specific concerns, and simplicity of model modification for system change, the STAMP model outperforms the OECD and CCPS models. This method, however, is still in its early stages, and industry professionals are unfamiliar with it. Low-level hazards that do not fit into any categories of unexpected events and hazardous control measures may have slipped out of the scope. Indicators can be developed at all organizational levels, such as top management, business area, facility, or specific activity. The analysis should include actors, preconditions, alternative processes, and non-functional requirements to improve the sophistication

of the study. More research can be conducted to improve the screening step to obtain adequate control with fewer indicators.

4.2 CONTRIBUTION TO PRACTICAL APPLICATION

This Ph.D. thesis contributes to applied research aimed at offshore and chemical process units with significant accident potential. *Table 3* presents an overview of the contribution of this thesis to practical application. As shown in the table, five contributions have been made, focusing on two industrial sectors, and the developed methods have been assessed for the below-mentioned industry challenges.

Table 3: Overview of the practical contribution of the theory developed in the thesis

Sector	Case study	Papers	Industrial challenge	Contribution to practical application
Process industry	Chemical production (Methyl Methacrylate.)	Paper IV	Finding inherently safer routes considering health, safety, and environment	Calculation of inherent safety to find a more inherently safer route
Oil and gas industry	LPG floating storage and regasification plant	Paper I	Proper hazard identification	Hazard identification using the SE method
		Paper V	Ensuring practical barriers for better risk control	Establishing an effective barrier strategy and safety assessment method
		Paper VI	Development of effective performance indicators	Development of indicators using the SE method

Paper IV's case study evaluates the inherent safety of several routes of Methyl Methacrylate manufacturing: via Acetone Cyanohydrin (ACH); via Ethylene and Propionaldehyde (C2/PA); via Ethylene and Methyl-Propionate (C2/MP), via Propylene (C3); via Tertiary butyl alcohol (TBA), and via Isobutene (iC4). The process flow of the route, along with the involved equipment and materials, were identified in the process. The state of each parameter, reaction temperature, pressure, process changes, and any recycling was also investigated. The case study can help other researchers select the best inherently safe route among different alternatives in other chemical products or processes.

Paper V assesses process safety barrier allocation and risk assessment for the LNG ship-to-ship transfer process. Establishing an improved safety barrier strategy can help the industry improve its risk management. Paper VI develops process safety indicators for LNG ship-to-ship transfer process system. A sound process safety management system can help the plant monitor its safety actions to address risk and improve accordingly. Paper I discusses the hazard identification of process leaks, an essential step in risk management for LNG floating storage and regasification units.

Hazard identification is discussed in detail with HAZOP and STPA procedures. The paper can benefit any industry personnel wanting detailed hazard identification for process industry applications and the LNG industry.

A system perspective allows a systematic and structured analysis, providing overall guidance. The entire work has investigated applying the SE process and theories in risk management. The system approach promotes and improves communication and supports the decision-making process among the different stakeholders.

5 CONCLUSION AND FURTHER WORKS

The research for this Ph.D. focused on improving risk management methodologies for automated systems and their applications in the petroleum and process industries. Massive interactions of new technologies, humans, and the environment are the challenges of today's digitalized system. The overall scientific objective of this thesis was to develop theories and methods for risk management of the modern automated plant. The goal was divided into four research sub-objectives related to hazard identification, inherently safer design, safety barriers allocation, and safety performance indicators. Sub objectives were achieved through six scientific papers. The four research questions in the thesis with brief answers were provided from the papers.

The first research question was whether present hazard identification methods are adequate for modern systems. An LNG ship-to-ship transfer case study explored two hazard identification methods, HAZOP and STPA. At the lowest level, the differences between the two strategies were negligible. Adopting STPA is that the analysis is very systematic and applicable to a socio-technical system. STPA necessitates the conduct of single research that covers all areas of errors. Creating a mitigation strategy and evaluating its success using control algorithms through scenario analysis is straightforward. The dynamic behavior of systems can be captured using STPA. The root situation can communicate the necessity for mitigation strategies at the broad level. The control diagram depicts incorrect or malicious system behavior and system losses at a higher level. HAZOP is better suited to any process containing simple interactions and minimal software because of its simplicity and shorter time requirements. STPA would be more appropriate for a complex system because it systematically detects dangers.

The issue with the second research question was how ISD could be improved. Present research work developed a parameter-based inherent system safety index to check the potentiality of inherent safety among design alternatives. The drawback of parameter-based indexing is that it selects fixed parameters that become invalid when the system changes or is extensively upgraded. The method starts by identifying the inherent safety characteristics of the system to overcome the drawback and identifying parameters related to those characteristics. Deviation scores were assigned for various parameters based on the hazard rating of each parameter. The interaction of various parameters raises the risk level at the operational stage. Various interactions were classified as 'vulnerability' parameters, and penalties were imposed. Different complexity criteria, such as equipment and number of streams, were recognized as potentially decreasing the system's comprehensibility and increasing the risk level. This method eliminates the dimensionality problem in calculating numerous subindices, a flaw in previous

parameter-based indexing systems. By identifying the individual issues more quickly, the design engineers will adapt the process to make it inherently safer.

The third research question was about how the method can be improved for better barrier allocation in the system. An extended FRAM method was applied to check the plant's safety barrier and safety assessment adequacy. Extended FRAM included a semi-quantitative approach to predict the performance of a system based on the performance of safety barriers. The method was applied for LNG ship-to-ship transfer operation, and comparisons were made among bowtie, FRAM-STPA, and Bayesian network. The analysis shows that the most dominant point in FRAM is that the method can consider the interaction between elements with time constraints, making it suitable for dynamic barrier management. Although the bowtie model is easy and requires a shorter time, a significant limitation is that it does not consider any interactions among multiple-barrier failures. The Bayesian network has a similar capability as FRAM regarding barrier management, for example, considering the coupling of multiple barriers changes in status with time. The only limitation is that the allocation of tasks or authority of tasks is not easily visible. The analysis gives insight into how small missing functions can lead to significant mishaps or performance deviations of plants from which analysts can benefit to ensure plant safety.

The last research question was how a safety performance indicator program could be established to ensure better risk management. The present research work investigated the STAMP accident model for developing performance indicators and compared the other two indicator development programs, OECD and CCPS. The research case study demonstrates that the STAMP model outperforms the OECD and CCPS in terms of early warning potential, area of emphasis, amount of detail in the study, ability to focus on specific concerns, and ease of model modification for a change in the system. Indicators can be created and used at various levels of an organization, including top management, business areas, facilities, and individual activities. However, because this concept is still new, industry professionals lack experience. Low-level hazards that do not fit into any of the categories of unexpected events as hazardous control activities may have been overlooked in the analysis. To increase the study's sophistication, it should incorporate actors, preconditions, alternative processes, and non-functional requirements.

Overall, the research focused improvement of risk management methods using a SE perspective. The current study emphasizes the development of simple, user-friendly approaches. One of the main limitations of systems thinking is the user's competence and communication among the stakeholders (Bucelli, 2020). Many models may emerge depending on the perspective utilized to frame and formulate a problem. As a result, participants' representations of the same system may be disproportionate. The research results open a broader view of the possible improvements instead of providing concrete solutions to all identified challenges. This research can be considered a prompt for more discussion and further research.

PROPOSAL FOR FURTHER RESEARCH

Based on the theory and methods developed in this thesis, several improvements can be made in the future in inherent safety evaluation, detailed hazard identification, improvement of barrier allocation, and performance monitoring. Details are described in this section.

System-based hazard identification

The study found that STPA is a powerful hazard identification method that can be effectively used in the process industry. Future work can be on the automation of STPA and combining risk quantification in STPA. There have been a few works on the automation of STPA, e.g., XSTAMP Plugin, Safety HAT project, Sahara, RM studio, STAMP workbench, and SpecTRM (Ludvigsen, 2018, Souza et al., 2019). They have the limitation of complexity, more ad-hoc, and limited functionalities. Further work can be done to develop user-friendly STPA software focusing on hazards relevant to the process and the petrochemical industry. Assessment of risk in STPA is qualitative. If the analyst wants to assess risk quantitatively, he must integrate another method with STPA. The architect of STPA, Leveson (2011), has argued that quantitative analysis in STPA is questionable for two reasons. Firstly, pursuing quantitative analysis can distract attention from critical causal factors that are not characterized statistically (Zhang et al., 2019). Secondly, it requires probabilistic insights about future events not supported by historical data. Assigning probabilistic information for loss scenarios is challenging and error-prone among system designers and experts (Zhang et al., 2019). Future work can be to add a quantification tool to the method by adopting features using a non-probabilistic model, keeping attention to causal factors as advised by Leveson.

Inherent system safety index

Inherent safety evaluation method, ISSI focuses only on evaluating inherent safety at the preliminary design or conceptual stage. Further research is necessary to extend the idea to make them applicable in the later stages of the plant and increase the calculation's sophistication. The inherent safety level of the system should also be checked when detailed data such as equipment sizing, auxiliary equipment, and process flowsheet are available in the detailed design stage. Issues raised at the detailed design stage, such as layout, structural integrity, and intermediate storage, were not included in the present model because it was developed focusing availability of parameters and data available at the concept development stage. The method can be modified to consider all the relevant parameters.

Temperature and pressure affect material properties (such as dispersion). Other operational parameters in the system may also affect the value. The model considers

a constant operational temperature (the maximum average temperature calculated from field data from a similar factory). Some parameters, such as the scale of recycling fuel gas used, were excluded from the established sub-index. Many interactions relevant to a chemical process were considered, such as ambient vapor pressure versus threshold limit value, while others were not. Many contradictory interactions of factors were ignored, such as the decrease in volatility when the boiling point rises. An extended model could be created to address these problems in the future. To keep the model simple, the research overlooked multiple events, such as a runaway reaction and several explosion mechanisms. A dynamic process simulation software (e.g., ASPEN HYSYS) can be coupled with the model to account for real-time data. Future work can improve the method's sophistication and remove its limitations. ISSI only considered the technical issues. Cost plays a vital role during the decision-making process. However, cost issues were not considered due to the limitation of the scope of work. Future work can be to optimize cost while evaluating inherent safety aspects.

System-based barrier allocation and risk assessment

A simple mathematical model was developed in the present research to check the system's safety performance using FRAM. Future work can be to conduct more case studies for other industrial cases with more complex systems. More effort can be made to improve the mathematical model's sophistication.

System-based performance indicator model

STAMP is a newer technique. More case studies should be conducted to assess the method's practicality and address practical application difficulties. The generation of indicators based on safety constraints is a difficult task. One constraint, for example, is that an operator must be aware of the proper operational procedures." What control actions measure that an operator is aware of the proper procedures, and how can they be implemented correctly? Supporting programs can be training programs for operators, internal quizzes, or tests to check the operator's competency, and correct documentation that the operator can follow. However, one may still ask if these are enough. A more straightforward direction should be included in the model to develop indicators from safety constraints.

Screening out of indicators from a considerable number of the list is also challenging. A risk estimation model can be integrated with the present model to check the risk level for violating safety constraints. Estimation of risk can guide choosing the most critical indicators for the process. A well-instructed guideline can be constructed in the future to achieve enough control with a lower number of indicators. The model's execution at the organizational level should be studied, and a framework needs to be developed. The research is conducted within the oil, gas, and chemical industry; evaluating other industries' methods will be attractive.

6 REFERENCES

ABDULKHALEQ, A. 2013. Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain Motivation: STAMP. *STPA Application Areas*, 1-17.

ABIDIN, M. Z., RUSLI, R., KHAN, F. & SHARIFF, A. M. 2018. Development of inherent safety benefits index to analyse the impact of inherent safety implementation. *Process Safety and Environmental Protection,* 117, 454-472.

ADE, N., LIU, G., AL-DOURI, A. F., EL-HALWAGI, M. M. & MANNAN, M. S. 2018. Investigating the effect of inherent safety principles on system reliability in process design. *Process safety and environmental protection,* 117, 100-110.

AHLUWALIA, A. & RUOCHEN, L. Managing blowout risk using a dynamic barrier approach. SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility, 2016. OnePetro.

AHMAD, S. I., HASHIM, H. & HASSIM, M. H. 2014. Numerical Descriptive Inherent Safety Technique (NuDIST) for inherent safety assessment in petrochemical industry. *Process Safety and Environmental Protection,* 92, 379-389.

AHMAD, S. I., HASHIM, H. & HASSIM, M. H. 2015. Graphical Technique for Root-Cause Analysis in Inherent Safety Assessment. *Advanced Materials Research,* 1113, 723.

AICHE & DOW 1987. *Fire & Explosion Index: Hazard Classification Guide*, Amer Inst of Chemical Engineers.

AMYOTTE, P. R., GORAYA, A. U., HENDERSHOT, D. C. & KHAN, F. I. 2007. Incorporation of inherent safety principles in process safety management. *Process Safety Progress,* 26, 333-346.

ANDOW, P., BRITAIN, H. G. & SAFETY, E. 1991. *Guidance on HAZOP procedures for computer-controlled plants*, Great Britain, Health and Safety Executive.

API, R. 2010. 754 Process Safety Performance Indicators for the Refining and Petrochemical Industries. *American Petroleum Institute, Washington DC*.

ATHAR, M., SHARIFF, A. M., BUANG, A. & HERMANSYAH, H. 2020. Equipment-based route index of inherent safety. *Process Safety Progress,* 39.

ATHAR, M., SHARIFF, A. M., BUANG, A., NAZIR, S., HERMANSYAH, H. & SEE, T. L. 2019. Process equipment common attributes for inherently safer process design at preliminary design stage. *Process Safety and Environmental Protection,* 128, 14-29.

AUST, J. & PONS, D. 2019. Bowtie Methodology for Risk Analysis of Visual Borescope Inspection during Aircraft Engine Maintenance. *Aerospace,* 6, 110.

AVEN, T. 2012. *Foundations of risk analysis*, John Wiley & Sons.

AVEN, T. 2016. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research,* 253, 1-13.

AVEN, T. & ZIO, E. 2014. Foundational issues in risk assessment and risk management. *Risk analysis,* 34, 1164-1172.

BAKER, R. D., WARREN, J. L., BEHMANESH, N. & ALLEN, D. T. 1992. Management of hazardous waste in the United States. *Hazardous waste and hazardous materials,* 9, 37-59.

BARTULOVIC, D. 2021. Predictive Safety Management System Development. *Transactions on Maritime Science,* 10**,** 1-12.
BAYBUTT, P. 2015. A critique of the Hazard and Operability (HAZOP) study. *Journal of Loss Prevention in the Process Industries,* 33**,** 52-58.
BELMONTE, F., SCHÖN, W., HEURLEY, L. & CAPEL, R. 2011. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway trafficsupervision. *Reliability Engineering & System Safety,* 96**,** 237-249.
BJERGA, T., AVEN, T. & ZIO, E. 2016. Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliability Engineering & System Safety,* 156**,** 203-209.
BOUTI, A. & KADI, D. A. 1994. A state-of-the-art review of FMEA/FMECA. *International Journal of reliability, quality and safety engineering,* 1**,** 515-543.
BRISTOW, M., FANG, L. & HIPEL, K. W. 2012. System of systems engineering and risk management of extreme events: Concepts and case study. *Risk Analysis: An International Journal,* 32**,** 1935-1955.
BRYMAN, A. 2016. *Social research methods*, Oxford university press.
BUCELLI, M. 2020. *Integrated Risk Management for Offshore Oil and Gas Installations.* Doctoral, NTNU.
BUDDE, S. F. 2012. *Modeling blowouts during drilling using STAMP and STPA.* Institutt for produksjons-og kvalitetsteknikk.
BURK, A. F. 1992. Strengthen process hazards reviews. *Chemical engineering progress,* 88**,** 90-94.
CAMERON, I. T., RAMAN, R. & RAMAN, R. 2005. *Process Systems Risk Management,* San Diego, San Diego: Elsevier Science & Technology.
CCPS 1993. *Guidelines for engineering design for process safety,* New York, Center for Chemical Process Safety of the American Institute of Chemical Engineers.
CCPS 2012. Process safety leading and lagging metrics. Center for Chemical Process Safety. AIChE, New York.
CCPS, A. 2007. Guidelines for risk based process safety. Hoboken, N.J.: Wiley-Interscience.
CHAHAL, P. & MOHAMMED, J. I. Assessment of Hazard Analysis and Implementation of STPA in Process Industry. Mary K O'Connor Process Safety Symposium. Proceedings 2019., 2019. Mary Kay O'Connor Process Safety Center.
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**,** 3236.
COX, L. A. 2009. *Risk Analysis of Complex and Uncertain Systems,* New York, NY, New York, NY: Springer-Verlag.
CRAWLEY, F. & TYLER, B. 2003. *Hazard identification methods*, IChemE.
CRAWLEY, F. & TYLER, B. 2015. *HAZOP: Guide to best practice*, Elsevier.
CRIVELLARI, A., BONVICINI, S., TUGNOLI, A. & COZZANI, V. 2021. Multi-target Inherent Safety Indices for the Early Design of Offshore Oil&Gas Facilities. *Process safety and environmental protection,* 148**,** 256-272.
DALLAT, C., SALMON, P. M. & GOODE, N. 2018. Identifying risks and emergent risks across sociotechnical systems: the NETworked hazard analysis and risk management system (NET-HARMS). *Theoretical issues in ergonomics science,* 19**,** 456-482.
DE CARVALHO, P. V. R. 2011. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic

management system resilience. *Reliability Engineering & System Safety,* 96**,** 1482-1498.
DE DIANOUS, V. & FIEVEZ, C. 2006. ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials,* 130**,** 220-233.
DORAN, J. & VAN DER GRAAF, G. Tripod-BETA: Incident investigation and analysis. SPE Health, Safety and Environment in Oil and Gas Exploration and Production Conference, 1996. OnePetro.
EDWARDS, D. W. & LAWRENCE, D. 1995. Assessing the inherent safety of chemical process routes. *Loss Prevention and Safety Promotion in the Process Industries, Vols 1 and 2***,** B473-B482.
ELLIS, G. R. & HOLT, A. A practical application of human-hazop for critical procedures. Hazards XXI Symposium Series, 2009. 434-439.
ERICSON, C. A. 2005. *Hazard Analysis Techniques for System Safety,* Hoboken, Hoboken: Wiley-Interscience.
FDIS, I. 2009. 31010: Risk Management—Risk Assessment Techniques. *IEC: Geneva, Switzerland*.
FRANK, M. V. 2010. *Choosing Safety: A guide to using probabilistic risk assessment and decision analysis in complex, high-consequence systems*, Routledge.
FREEMAN, P. W., MEARNS, A. B., SLANA, M. F. & BELL TELEPHONE, L. 1966. *Fault tree analysis : the study of unlikely events in complex systems,* S.l.
FUKUDA, K., SAWARAGI, T., HORIGUCHI, Y. & NAKANISHI, H. 2016. Applying Systemic Accident Model to Learn from Near-Miss Incidents of Train Maneuvering and Operation. *IFAC-PapersOnLine,* 49**,** 543-548.
FUSSELL, J. 1975. A review of fault tree analysis with emphasis on limitations. *IFAC Proceedings Volumes,* 8**,** 552-557.
GANGADHARAN, P., SINGH, R., CHENG, F. Q. & LOU, H. H. 2013. Novel Methodology for Inherent Safety Assessment in the Process Design Stage. *Industrial & Engineering Chemistry Research,* 52**,** 5921-5933.
GAO, X., RAMAN, A. A. A., HIZADDIN, H. F., BELLO, M. M. & BUTHIYAPPAN, A. 2021. Review on the Inherently Safer Design for Chemical Processes: Past, Present and Future. *Journal of Cleaner Production***,** 127154.
GARBOLINO, E., BOULOIZ, H., HARDY, K., OUEIDAT, D. & SAMADI, J. 2019. *Safety Dynamics: Evaluating Risk in Complex Industrial Systems*, Springer International Publishing.
GARVEY, P. R. 2008. *Analytical methods for risk management: A systems engineering perspective*, Crc Press.
GROOT, A. Advanced process safety barrier management by applying proactive incident investigation to failed or impaired barriers. SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility, 2016. OnePetro.
GROSE, V. System safety education focused on system management(Methodological approach to managing system safety). NASA, Washington Govt.-Ind. System Safety Conf. p 113-126(SEE N 72-25961 16-34), 1971.
GROSSEL, S. S. 1993. Guidelines for Hazard Evaluation Procedures, with Worked Examples: Center for Chemical Process SafetyCenter for Chemical Process Safety of the American Institute of Chemical Engineers, New York, 1992, 461 pages, ISBN 0 816 904 91X. Elsevier.

GRØTAN, T. & PALTRINIERI, N. 2016. Dynamic risk management in the perspective of a resilient system. *Dynamic Risk Analysis in the Chemical and Petroleum Industry.* Elsevier.
GUARNIERI, F., GARBOLINO, E., BOULOIZ, H., HARDY, K., OUEIDAT, D. & SAMADI, J. 2019. *Safety Dynamics*, Springer.
GUNASEKERA, M. & EDWARDS, D. 2006. Chemical process route selection based upon the potential toxic impact on the aquatic, terrestrial and atmospheric environments. *Journal of Loss Prevention in the Process Industries,* 19**,** 60-69.
GUPTA, J. & EDWARDS, D. W. 2003. A simple graphical method for measuring inherent safety. *Journal of Hazardous Materials,* 104**,** 15-30.
GUPTA, J. P., KHEMANI, G. & MANNAN, M. S. 2003. Calculation of Fire and Explosion Index (F&EI) value for the Dow Guide taking credit for the loss control measures. *Journal of Loss Prevention in the Process Industries,* 16**,** 235-241.
HALE, A. 2009. Why safety performance indicators? *Safety Science,* 4**,** 479-480.
HAM, D.-H. 2020. Safety-II and resilience engineering in a nutshell: an introductory guide to their concepts and methods. *Safety and health at work*.
HAM, D.-H. 2021. Safety-II and Resilience Engineering in a Nutshell: An Introductory Guide to Their Concepts and Methods. *Safety and Health at Work,* 12**,** 10-19.
HAMMER, W. Why system safety programs can fail. NASA, Washington Govt.-Ind. System Safety Conf., 1971.
HANESS, S. J. & WARWICK, J. J. 1991. Evaluating the hazard ranking system. *Journal of environmental management,* 32**,** 165-176.
HASKINS, C., FORSBERG, K., KRUEGER, M., WALDEN, D. & HAMELIN, D. Systems engineering handbook. INCOSE, 2006. 13-16.
HASSIM, M. & EDWARDS, D. 2006. Development of a methodology for assessing inherent occupational health hazards. *Process Safety and Environmental Protection,* 84**,** 378-390.
HATAYAMA, H. 1980. *A method for determining the compatibility of hazardous wastes*, Environmental Protection Agency, Office of Research and Development ….
HEIKKILÄ, A.-M. 1999. *Inherent safety in process plant design: an index-based approach*, VTT Technical Research Centre of Finland.
HEINEMANN, H. 1979. A brief history of industrial catalysis. Lawrence Berkeley National Lab.(LBNL), Berkeley, CA (United States).
HEINRICH, H. W. 1941. Industrial Accident Prevention. A Scientific Approach. *Industrial Accident Prevention. A Scientific Approach.*
HERRERA, I. A., HOLLNAGEL, E. & HÅBREKKE, S. Proposing safety performance indicators for helicopter offshore on the Norwegian Continental Shelf. PSAM 10-Tenth Conference on Probabilistic Safety Assessment and Management, 2010. 10.
HOEL, F. 2012. *Modeling process leaks offshore using STAMP and STPA.* Institutt for produksjons-og kvalitetsteknikk.
HOEPFFNER, L. 1989. Analysis of the HAZOP study and comparison with similar safety analysis systems. *Gas Separation & Purification,* 3**,** 148-151.
HOLLNAGEL, E. 2016. *Barriers and accident prevention*, Routledge.
HOLLNAGEL, E. 2017. *FRAM: the functional resonance analysis method: modelling complex socio-technical systems*, CRC Press.
HOSSEINNIA DAVATGAR, B., PALTRINIERI, N. & BUBBICO, R. 2021. Safety barrier management: risk-based approach for the oil and gas sector. *Journal of Marine Science and Engineering,* 9**,** 722.

HOSSEINNIAA, B., HASKINSA, C., RENIERSB, G. & PALTRINIERIA, N. 2019. A guideline for the dynamic barrier management framework based on system thinking. *CHEMICAL ENGINEERING,* 77.
HSE 2006. Developing Process Safety Indicators—A Step-By-Step Guide for Chemical and Major Hazard Industries. *Health and Safety Executive, UK*.
HULIN, B. & TSCHACHTLI, R. 2011. Identifying software hazards with a modified CHAZOP. *Proceedings of the PESARO2011, Budapest, Hungary*, 17-22.
HYSYS, A. 1995. V7. 3; Aspen Technology, Inc. *Burlington, MA,* 2011.
IEC 2001. Hazard and Operability Studies (HAZOP Studies)-Application Guide-BS IEC 61882.
IEC 2003. Functional safety-Safety instrumented systems for the process industry sector. *IEC 61511-3*.
IEC 2010. Functional safety of electrical/electronic/programmable electronic safety-related systems: IEC 61508. CENELEC.
INSTONE, B. Losses in the hydrocarbon process industries. Proceedings of 6th Int. Symposium Loss Prevention and Safety Promotion in the Chemical Industries, Oslo, 1989. 118-119.
ISO 2010. Petroleum and natural gas industries - Drilling and production equipment - Subsurface barrier valves and related equipment. *ISO 10423.* ISO/TC 67/SC 4.
ISO 2015. Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines-ISO 13702. ISO.
JAFARI, M. J., MOHAMMADI, H., RENIERS, G., POUYAKIAN, M., NOURAI, F., TORABI, S. A. & MIANDASHTI, M. R. 2018. Exploring inherent process safety indicators and approaches for their estimation: A systematic review. *Journal of Loss Prevention in the Process Industries,* 52, 66-80.
JANSEN, B. & FIRING, F. A holistic approach to safety barrier management. SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility, 2016. OnePetro.
JANSSENS, J., TALARICO, L., RENIERS, G. & SÖRENSEN, K. 2015. A decision model to allocate protective safety barriers and mitigate domino effects. *Reliability engineering & system safety,* 143, 44-52.
JENNINGS, K. & SCHULBERG, F. Oecd Guidance on Safety Performance Indicators. The 2007 Spring National Meeting, 2007.
JENSEN, A. 2018. *Contributions to hazard/threat identification and analysis in complex systems.* no. 408, Faculty of Science and Technology, University of Stavanger, .
KAMRANI, A. K. & AZIMI, M. 2011. Systems engineering tools and methods. Boca Raton: CRC Press.
KANG, J., ZHANG, J. & GAO, J. 2009. Analysis of the safety barrier function: Accidents caused by the failure of safety barriers and quantitative evaluation of their performance. *Journal of loss prevention in the process industries,* 43, 361-371.
KARANIKAS, N. & ABRINI, M. Using STPA for evaluating aviation safety management systems. STAMP Workshop 2016, 2016.
KAVIANIAN, H. R. 1992. *Application of hazard evaluation techniques to the design of potentially hazardous industrial chemical processes*, US Department of Health and Human Services, Public Health Service, Centers
KHAKZAD, N., KHAN, F. & AMYOTTE, P. 2012. Dynamic risk analysis using bow-tie approach. *Reliability Engineering & System Safety,* 104, 36-44.

KHAN, F. I. & ABBASI, S. 1998a. Techniques and methodologies for risk analysis in chemical process industries. *Journal of loss Prevention in the Process Industries,* 11**,** 261-277.
KHAN, F. I. & ABBASI, S. A. 1998b. Inherently safer design based on rapid risk analysis. *Journal of Loss Prevention in the Process Industries,* 11**,** 361-372.
KHAN, F. I. & AMYOTTE, P. R. 2002. Inherent safety in offshore oil and gas activities: a review of the present status and future directions. *Journal of Loss Prevention in the Process Industries,* 15**,** 279-289.
KHAN, F. I. & AMYOTTE, P. R. 2004. Integrated inherent safety index (12SI): A tool for inherent safety evaluation. *Process Safety Progress,* 23**,** 136-148.
KHAN, F. I., HUSAIN, T. & ABBASI, S. A. 2001. Safety weighted hazard index (SWeHI): a new, user-friendly tool for swift yet comprehensive hazard identification and safety evaluation in chemical process industrie. *Process Safety and Environmental Protection,* 79**,** 65-80.
KING, R. 2016. *Safety in the process industries*, Elsevier.
KLETZ 2010. Process Plants: A Handbook for Inherently Safer Design. Hoboken.
KLETZ, T. 1985. Make plants inherently safe. *Hydrocarbon Process.;(United States),* 64.
KLETZ, T. 2018. *HAZOP and HAZAN: identifying and assessing process industry hazards*, CRC Press.
KLETZ, T. A. 1991. Inherently Safer Plants - Recent Progress. *Hazards Xi : New Directions in Process Safety***,** 225-233.
KLETZ, T. A. 1995. Inherently safer design - The growth of an idea. *Lps 1995 - Proceedings of the 29th Annual Loss Prevention Symposium***,** 1-11.
KLETZ, T. A. 1999. The constraints on inherently safer design and other innovations. *Process Safety Progress,* 18**,** 64-69.
KLETZ, T. A. 2003. Inherently safer design—its scope and future. *Process Safety and Environmental Protection,* 81**,** 401-405.
KLUGMANN-RADZIEMSKA, E. Environmental impacts of renewable energy technologies. Int Conf Environ Sci Technol. IPCBEE, Singapore, 2014. 104-109.
KOTHARI, C. R. 2004. *Research methodology: Methods and techniques*, New Age International.
LAPORTE, T. R. & CONSOLINI, P. M. 1991. Working in practice but not in theory: theoretical challenges of" high-reliability organizations". *Journal of Public Administration Research and Theory: J-PART,* 1**,** 19-48.
LAURA, M. O. D. & JAMES, A. B. 2014. *Quantitative Research for the Qualitative Researcher,* Los Angeles, SAGE Publications, Inc.
LAWLEY, H. 1974. Operability studies and hazard analysis. *Chem. Eng. Prog.,* 70**,** 45-56.
LAWRENCE, D. 1996. *Quantifying inherent safety of chemical process routes.* Doctoral dissertation, Loughborough University.
LAWRENCE, D. & EDWARDS, D. W. 1994. Inherent Safety Assessment of Chemical Process Routes by Expert Judgement. *1994 Icheme Research Event, Vols 1 and 2***,** 886-888.
LEE, W.-S., GROSH, D. L., TILLMAN, F. A. & LIE, C. H. 1985. Fault tree analysis, methods, and applications ๏ a review. *IEEE transactions on reliability,* 34**,** 194-203.
LEES, F. 2012. *Lees' Loss prevention in the process industries: Hazard identification, assessment and control*, Butterworth-Heinemann.
LEONG, C. T. & SHARIFF, A. M. 2008. Inherent safety index module (ISIM) to assess inherent safety level during preliminary design stage. *Process Safety and Environmental Protection,* 86**,** 113-119.

LEONG, C. T. & SHARIFF, A. M. 2009. Process route index (PRI) to assess level of explosiveness for inherent safety quantification. *Journal of Loss Prevention in the Process Industries,* 22**,** 216-221.
LEVENSON, N. G. 1995. *System safety and computers*, Addison Wesley.
LEVESON, N. 2004. A new accident model for engineering safer systems. *Safety science,* 42**,** 237-270.
LEVESON, N. 2011. *Engineering a safer world: Systems thinking applied to safety*, MIT press.
LEVESON, N. G. Using STAMP to Develop Leading Indicators. GI-Jahrestagung, 2014. 597-600.
LEWIS, D. The Mond Fire, Explosion and Toxicity Index-a Development of the Dow Index. Proceedings of the AIChE on loss prevention symposium, New York, 1979.
LI, J. H., HUANG, Z. H. & LI, S. J. 2008. Application of Mond Fire Explosion and Toxicity Index Evaluation Method in H(2)S Tanks. *Progress in Safety Science and Technology, Vol Vii, Pts a and B,* 7**,** 233-237.
LI, K., YAO, X., CHEN, D., YUAN, L. & ZHOU, D. 2014. HAZOP study on the CTCS-3 onboard system. *IEEE Transactions on Intelligent Transportation Systems,* 16**,** 162-171.
LI, X. A., ZANWAR, A., JAYSWAL, A., LOU, H. H. & HUANG, Y. L. 2011. Incorporating Exergy Analysis and Inherent Safety Analysis for Sustainability Assessment of Biofuels. *Industrial & Engineering Chemistry Research,* 50**,** 2981-2993.
LUDVIGSEN, N. 2018. *Prototyping a digital support tool for an agile implementation of STPA.* Master's thesis, , NTNU.
MACDONALD, D. 2003. *Practical Industrial Safety, Risk Assessment and Shutdown Systems,* Oxford, Elsevier Science & Technology.
MACDONALD, D. 2004. *Practical Hazops, Trips and Alarms,* Oxford, Elsevier Science & Technology.
MANNAN, S. 2014. *Lees' process safety essentials : hazard identification, assessment and control,* Amsterdam, Elsevier/Butterworth-Heinemann.
MARCH, J. G. 1994. *Primer on decision making: How decisions happen*, Simon and Schuster.
MCLUCAS, A. C. 2003. *Decision making: risk management, systems thinking and situation awareness*, Argos Press P/L.
MILES, M. B. & HUBERMAN, A. M. 1994. *Qualitative data analysis: An expanded sourcebook*, Sage publications.
MOORE, D. A. 2003. The regulation of inherent safety. *Hazards Xvii: Process Safety - Fulfilling Our Responsibilities***,** 247-256.
MOSHER, G. A. & KEREN, N. Analysis of safety decision-making data using event tree analysis. 2011 Agricultural and Biosystems Engineering. Iowa State University.
MÖLLER, N. 2012. The concepts of risk and safety. *Handbook of risk theory: epistemology, decision theory, ethics, and social implications of risk,* 1**,** 55-85.
MÅRTENSSON, P., FORS, U., WALLIN, S.-B., ZANDER, U. & NILSSON, G. H. 2016. Evaluating research: A multidisciplinary approach to assessing research practice and quality. *Research Policy,* 45**,** 593-603.
NAKAO, H., KATAHIRA, M., MIYAMOTO, Y. & LEVESON, N. Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. Proc. of the 5: th IAASS Conference, 2011. Citeseer, 497-501.

NELSON, W. R. Decision Support for Dynamic Barrier Management: Enhancing Safety and Regulatory Compliance Assessment for Offshore Operations. SPE Mexico Health, Safety, Environment, and Sustainability Symposium, 2016. OnePetro.
NETO, F. C., RIBEIRO, J., UGULINO, K. & MINGRONE, S. 2014. Safety barriers integrity management system. *Chemical Engineering Transactions,* 36**,** 493-498.
NFPA 2017. *NFPA 704, Standard System for the Identification of the Hazards of Materials for Emergency Response*, National Fire Protection Association.
NICHOLAS, J. 2017. *System Safety Engineering and Risk Assessment: A Practical Approach*, CRC Press.
NIELSEN, D. S. 1971. *The cause/consequence diagram method as a basis for quantitative accident analysis*, Risø National Laboratory.
NISKANEN, T. 2018. A Resilience Engineering -related approach applying a taxonomy analysis to a survey examining the prevention of risks. *Safety Science,* 101**,** 108-120.
OECD 2003. *OECD Guidance on Safety Performance Indicators : A Companion to the OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response,* Paris, Organisation for Economic Co-operation and Development.
OSHA 1983. *General industry : OSHA safety and health standards (29 CFR 1910),* Washington, D.C, OSHA.
OSMUNDSEN, P., AVEN, T. & VINNEM, J. E. 2008. Safety, economic incentives and insurance in the Norwegian petroleum industry. *Reliability Engineering & System Safety,* 93**,** 137-143.
OXFORD 1989. Dictionary, Oxford English & Idioms, English. Oxford references online: Oxford University Press.
PALANIAPPAN, C., SRINIVASAN, R. & TAN, R. 2002. Expert system for the design of inherently safer processes. 1. Route selection stage. *Industrial & engineering chemistry research,* 41**,** 6698-6710.
PALTRINIERI, N. 2016. *Dynamic Risk Analysis in the Chemical and Petroleum Industry: Evolution and Interaction with Parallel Disciplines in the Perspective of Industrial Application,* San Diego, CA, USA, San Diego, CA, USA: Elsevier Science.
PALTRINIERI, N., KHAN, F., AMYOTTE, P. & COZZANI, V. 2014. Dynamic approach to risk management: Application to the Hoeganaes metal dust accidents. *Process Safety and Environmental Protection,* 92**,** 669-679.
PASMAN, H. 2015. Sociotechnical Systems, System Safety, Resilience Engineering, and Deeper Accident Analysis. *Risk Analysis and Control for Industrial Processes - Gas, Oil and Chemicals.*
PERROW, C. 2011. *Normal accidents*, Princeton university press.
PEZESHKI, S. I. 2020. *Functional Resonance Analysis Method (FRAM) Approach for Barrier Management in Offshore Drilling.* Master's thesis, NTNU.
PITBLADO, R., FISHER, M., NELSON, B., FLØTAKER, H., MOLAZEMI, K. & STOKKE, A. 2016. Concepts for dynamic barrier management. *Journal of loss prevention in the process industries,* 43**,** 741-746.
PLANAS-CUCHI, E., MONTIEL, H. & CASAL, J. 1997. A Survey of the Origin, Type and Consequences of Fire Accidents in Process Plants and in the Transportation of Hazardous Materials. *Process safety and environmental protection,* 75**,** 3-8.
PLIOUTSIAS, A. & KARANIKAS, N. 2015. Using STPA in the evaluation of fighter pilots training programs. *Procedia Engineering,* 128**,** 25-34.
POPE, W. 1971. System safety management: A new discipline. *NASA, Washington Govt.-Ind. System safety Conference.*

RAHMAN, M., HEIKKILA, A. M. & HURME, M. 2005. Comparison of inherent safety indices in process concept evaluation. *Journal of Loss Prevention in the Process Industries,* 18**,** 327-334.
RAMZALI, N., LAVASANI, M. R. M. & GHODOUSI, J. 2015. Safety barriers analysis of offshore drilling system by employing fuzzy event tree analysis. *Safety science,* 78**,** 49-59.
RANASINGHE, U., JEFFERIES, M., DAVIS, P. & PILLAY, M. 2020. Resilience Engineering Indicators and Safety Management: A Systematic Review. *Safety and health at work,* 11**,** 127-135.
RASMUSSEN, J. 1997. Risk management in a dynamic society: a modelling problem. *Safety science,* 27**,** 183-213.
RATHNAYAKA, S., KHAN, F. & AMYOTTE, P. 2014. Risk-based process plant design considering inherent safety. *Safety Science,* 70**,** 438-464.
RAUSAND, M. 2005. Preliminary hazard analysis. Department of Production and Quality Engineering, Norwegian University of Science and Technology.
RAUSAND, M. 2011. *Risk Assessment: Theory, Methods, and Applications,* Somerset, Somerset: John Wiley & Sons, Incorporated.
REASON, J. 1997. *Managing the risks of organizational accidents*, Routledge.
REDMILL, F., CHUDLEIGH, M. & CATMUR, J. 1999. *System safety : HAZOP and software HAZOP,* Chichester, Wiley.
REJZEK, M. & HILBES, C. 2018. Use of STPA as a diverse analysis method for optimization and design verification of digital instrumentation and control systems in nuclear power plants. *Nuclear Engineering and Design,* 331**,** 125-135.
RENIERS, G. L., ALE, B., DULLAERT, W. & SOUDAN, K. 2009. Designing continuous safety improvement within chemical industrial areas. *Safety Science,* 47**,** 578-590.
RODRIGUEZ, M. & DIAZ, I. 2016. A systematic and integral hazards analysis technique applied to the process industry. *Journal of Loss Prevention in the Process Industries,* 43**,** 721-729.
ROLAND, H. E. & MORIARTY, B. 1990. System safety engineering and management. John Wiley & Sons.
ROSENFELD, P. E. & FENG, L. 2011. *Risks of hazardous wastes*, William Andrew.
ROSNESS, R., GUTTORMSEN, G., STEIRO, T., TINMANNSVIK, R. K. & HERRERA, I. A. 2010. Organisational Accidents and Resilient Organisations: Six Perspectives *Trondheim: SINTEF Industrial Management,* 2.
RUSLI, R. & SHARIFF, A. M. 2010. Qualitative assessment for inherently safer design (QAISD) at preliminary design stage. *Journal of Loss Prevention in the Process Industries,* 23**,** 157-165.
SAUNDERS, R. 1992. *The safety audit : designing effective strategies,* London, Pitman Publ.
SHARIFF, A. M. & LEONG, C. T. 2009. Inherent risk assessment-A new concept to evaluate risk in preliminary design stage. *Process Safety and Environmental Protection,* 87**,** 371-376.
SHARIFF, A. M., LEONG, C. T. & ZAINI, D. 2012. Using process stream index (PSI) to assess inherent safety level during preliminary design stage. *Safety science,* 50**,** 1098-1103.
SHARIFF, A. M., RUSLI, R., LEONG, C. T., RADHAKRISHNAN, V. R. & BUANG, A. 2006. Inherent safety tool for explosion consequences study. *Journal of Loss Prevention in the Process Industries,* 19**,** 409-418.
SHARIFF, A. M. & ZAINI, D. 2010. Toxic release consequence analysis tool (TORCAT) for inherently safer design plant. *Journal of hazardous materials,* 182**,** 394-402.

SINGH, J. & MUNDAY, G. IFAL: a model for the evaluation of chemical process losses. Design 79 Symposium. Institute of Chemical Engineering Midlands Branch London, 1979.
SKLET, S. 2006. Safety barriers: Definition, classification, and performance. *Journal of loss prevention in the process industries,* 19**,** 494-506.
SKLET, S. & HAUGE, S. 2004. Safety barriers to prevent release of hydrocarbons during production of oil and gas. *SINTEF Rapport*.
SMITH, D., VEITCH, B., KHAN, F. & TAYLOR, R. 2017. Understanding industrial safety: Comparing Fault tree, Bayesian network, and FRAM approaches. *Journal of Loss Prevention in the Process Industries,* 45**,** 88-101.
SOBRAL, J. & SOARES, C. G. 2019. Assessment of the adequacy of safety barriers to hazards. *Safety science,* 114**,** 40-48.
SONG, D., YOON, E. S. & JANG, N. 2018. A framework and method for the assessment of inherent safety to enhance sustainability in conceptual chemical process design. *Journal of Loss Prevention in the Process Industries,* 54**,** 10-17.
SOUZA, F., PEREIRA, D., MARTINS PAGLIARES, R., NADJM-TEHRANI, S. & HIRATA, C. 2019. WebSTAMP: a Web Application for STPA & STPA-Sec. *MATEC Web of Conferences,* 273**,** 02010.
STAMATIS, D. H. 2003. *Failure mode and effect analysis: FMEA from theory to execution*, Quality Press.
STEEN, R. & AVEN, T. 2011. A risk perspective suitable for resilience engineering. *Safety Science,* 49**,** 292-297.
SULTANA, S., ANDERSEN, B. S. & HAUGEN, S. 2019a. Identifying safety indicators for safety performance measurement using a system engineering approach. *Process Safety and Environmental Protection,* 128**,** 107-120.
SULTANA, S., BUCHELI, M., ZHANG, J. & RAUZY, A. How system engineering may be helpful in preparing fmeca - lesson learnt from a practical case. European Safety and Reliability Conference, 2018 Trondheim, Norway.
SULTANA, S. & HAUGEN, S. Achieving inherent safety from inherent hazard and risk factors European Safety and Reliability Conference, 2021 France.
SULTANA, S. & HAUGEN, S. 2022. Development of an inherent system safety index (ISSI) for ranking of chemical processes at the concept development stage. *Journal of Hazardous Materials,* 421**,** 126590.
SULTANA, S., OKOH, P., HAUGEN, S. & VINNEM, J. E. 2019b. Hazard analysis: Application of STPA to ship-to-ship transfer of LNG. *Journal of Loss Prevention in the Process Industries,* 60**,** 241-252.
SULTANA, S., VINNEM, J. E., DAHLSVEEN, J. & HAUGEN, S. Inherent safety assessment: current state of the art and why is still not effectively adopted by industry. 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, 2020 Italy. Research Publishing, Singapore.
SUMMERS, A. 2018. Inherently Safer Automation. *Process Safety Progress,* 37**,** 31-36.
TOGHRAEI, M. 2019. *Piping and Instrumentation Diagram Development*, John Wiley & Sons.
TROCHIM, W. M. & DONNELLY, J. P. 2001. *Research methods knowledge base*, Atomic Dog Pub.
TYLER, B. 1985. Using the Mond Index to measure inherent hazards. *Process Safety Progress,* 4**,** 172-175.
VALDEZ BANDA, O. A. & GOERLANDT, F. 2018. A STAMP-based approach for designing maritime safety management systems. *Safety science,* 109**,** 109-129.

VAN SCYOC, K. 2008. Process safety improvement—Quality and target zero. *Journal of hazardous materials,* 159**,** 42-48.
VARDE, P. V. & PECHT, M. G. 2018. Risk-Based Engineering : An Integrated Approach to Complex Systems—Special Reference to Nuclear Plants. 1st ed. 2018. ed. Singapore: Springer Singapore : Imprint: Springer.
VAZQUEZ, D., RUIZ-FEMENIA, R. & CABALLERO, J. A. 2019. OFISI, a novel optimizable inherent safety index based on fuzzy logic. *Computers & Chemical Engineering,* 129.
VISSCHER, G. Some observations about major chemical accidents from recent CSB investigations. Institution of chemical engineers symposium series, 2008. Institution of Chemical Engineers; 1999, 34.
WEICK, K. E. & SUTCLIFFE, K. M. 2001. *Managing the unexpected*, San Francisco: Jossey-Bass.
WELLS, G. 1997. *Hazard identification and risk assessment*, IChemE.
WILLEY, R. J. 2014. Layer of protection analysis. *Procedia Engineering,* 84**,** 12-22.
WOODS, D. & WREATHALL, J. 2003. Managing risk proactively: the emergence of resilience engineering. *Columbus: Ohio University*.
XIE, L., LUNDTEIGEN, M. A. & LIU, Y. 2018. Safety barriers against common cause failure and cascading failure: literature reviews and modeling strategies. Institute of Electrical and Electronics Engineers (IEEE).
YEO, C., BHANDARI, J., ABBASSI, R., GARANIYA, V., CHAI, S. & SHOMALI, B. 2016. Dynamic risk analysis of offloading process in floating liquefied natural gas (FLNG) platform using Bayesian Network. *Journal of Loss Prevention in the Process Industries,* 41**,** 259-269.
YIN, R. K. 2011. *Applications of case study research*, Sage publications.
ZHANG, J., KIM, H., LIU, Y. & LUNDTEIGEN, M. A. 2019. Combining system-theoretic process analysis and availability assessment: A subsea case study. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* 233**,** 520-536.
ÅRSTAD, I. 2019. *Preventing major accidents : - conditions for prudence.* no. 440, University of Stavanger, Faculty of Science and Technology, Risk Management and Social Safety.

Paper I

Sultana, S., Vinnem J.E., Okoh P., & Vinnem, J. E., (2019). Hazard analysis: Application of STPA to the ship-to-ship transfer of LNG Journal of Loss Prevention in the Process Industries, 60, 241-252

Journal of Loss Prevention in the Process Industries 60 (2019) 241–252

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Hazard analysis: Application of STPA to ship-to-ship transfer of LNG

Sharmin Sultana[a,*], Peter Okoh[b], Stein Haugen[a], Jan Erik Vinnem[a]

[a] Department of Marine Technology, Norwegian University of Science & Technology, NTNU, Norway
[b] Department of Engineering Cybernetics, Norwegian University of Science & Technology, NTNU, Norway

ABSTRACT

The process industry has experienced technological advances, such as automatic handling of hazardous substances, process equipment, and valves. High levels of automation, as well as system interactions at component and system levels, have brought new challenges to risk management. A modern process system involves multiple controllers. Even if each controller can control the process individually, an unexpected event may occur due to unintended interactions or insufficient attention to safety requirements and constraints. Recent accidents in Plymouth, UK, and Nigeria have attracted the attention of scientists, who have concluded that approaches currently being used are insufficient. A traditional hazard analysis tool, such as Hazard and Operability Studies (HAZOP) or simple reliability analysis methods such as Failure Mode and Effect Analysis (FMEA) cannot investigate the lack of complex systems properly. System Theoretical Process Analysis (STPA) is established to evaluate the safety of such complex systems. It has been used successfully in automated missiles and driving vehicles. However, the use of STPA in process industry applications is scarce. This paper is written to evaluate the feasibility of using STPA in process industry applications. A comparative analysis is conducted between STPA and HAZOP to determine whether STPA can replace traditional HAZOP or not with the help of a case study: Liquefied Natural Gas (LNG) Ship-to-Ship (STS) transfer. The results of the analysis show that STPA is complementary to traditional HAZOP. However, this conclusion is drawn based on only one specific case study (LNG STS transfer) and requires further analysis of other process applications for validation.

1. Introduction

With the introduction of new technology, modern process systems are facing new safety challenges. Systems have become more software-intensive and are composed not only of hardware components but also logic control devices, software and an increasing number of sensors. Human intervention in certain situations is still unavoidable, and the human-machine interface is always a challenge. In these systems, accidents occur not only due to hardware failure, but also due to software failure, interaction problems between components and controllers (Kletz, 1995; Abdulkhaleq et al., 2017) and error or delay in data entry into the computer.

The BP Deepwater Horizon explosion (Eargle and Esmail, 2012), the fire in the MLGN Tiga project (Mayer et al., 2003), the steam boiler explosion in Skikda Algeria (Ouddai et al., 2012), the LNG accident in Plymouth (Wutc, 2016), and the LNG pipeline explosion in Nigeria (Saheed and Egwaikhide, 2012) have attracted the attention of researchers. They addressed the need for new methods which can eliminate the system flaws related to such accidents. The fire that occurred in the Petronas' LNG complex in the MLNG Tiga project at Bintulu, Malaysia, in 2003 was in the exhaust system of a propane gas turbine. According to the investigation committee, the complexity of equipment, lack of adequate surveillance, lack of integrity of organizational processes and issues with the safety management system (Othman et al., 2014) were contributing reasons for the accident of having adequate inspection plan. In Skikda, Algeria, in 2004, in the LNG production plant, a steam boiler explosion caused a massive vapor cloud including fire.

The accident caused 27 deaths, 74 injuries and damage to a large section of the LNG plant. The accident is reported to have occurred due to poor maintenance, poor site management, lack of accident prevention and improper communication of safety policy (Ouddai et al., 2012). In Nigeria, in 2005, the LNG underground pipeline explosion caused a massive fire that spread over a large area. The accident occurred due to the negligence of personnel during operation or inadequate maintenance (Khan and Abbasi, 1999). In the investigation of the Plymouth accident, reveals that organizational factors, which the company had not resolved before the accident, were primary contributors. According to Paltrinieri et al. (2015), new disasters require new accident prevention scenarios evolving from innovative technologies, which existing traditional methods are unable to identify. Other recent LNG accidents also draw attention to the fact that human organizational factors, such as miscommunication, lack of integrity of the regulatory process, reduced maintenance, and lack of training for emergency responders contributed to the most of these accidents.

HAZOP (Crawley and Tyler), CHazop, fault tree analysis (Barlow and Chatterjee, 1973) and Failure Mode and Effect Criticality Analysis (FMECA) (AMES Research, 1973), have been used widely for hazard

* Corresponding author.
E-mail address: sharmin.sultana@ntnu.no (S. Sultana).

https://doi.org/10.1016/j.jlp.2019.04.005
Received 2 May 2018; Received in revised form 5 February 2019; Accepted 4 April 2019
Available online 09 April 2019
0950-4230/

analysis in the process industry for a long time. FMECA evaluates the effect of individual component failures on system performance (Stamatis, 2003). FMECA identifies essential causes of failures like component interactions or software errors but does not emphasize the operational context (Stamatis, 2003). CHazop is developed to identify potential hazards and operability problems in control and computer systems. However, standardized CHazop does not exist. There are various CHazop procedures; yet, none of them have been validated to be considered good engineering practice. CHazop is said to have four technical insufficiencies: Ambiguity, incompleteness, nonsensicality, and redundancy (Hulin and Tschachtli, 2011).

Traditional risk analysis methods assume accidents as a result of component failures or faults (Marais et al., 2004) and oversimplify the role of humans (Leveson, 2011b). These methods are successful in evaluating design flaws in simple linear process systems. For complex interconnected systems, these methods are insufficient and cannot capture the entire accident process (Rokseth et al., 2017). In traditional risk assessment, there is a tendency to assert that designed systems are safe enough, rather than modifying the designed system from a safety point of view (Drogoul et al., 2005). In case of identification of system deficiencies at a later stage, reassessment requires a redesign from initial stages, increasing cost and time.

Risk analysis of modern process systems should not focus only on component failure but also on software errors, controller interaction problems, and coordination problems in decision making. System-focused risk analysis methods look promising amidst the rapid evolution of technology. Today's risk assessment should include environmental issues, software design error, human error, late decision-making problems, and coordination inadequacy.

Researchers have STPA has been applied in different domains, e.g., security (Young and Leveson, 2014), software safety (Abdulkhaleq et al., 2015), in the aviation industry (Leveson, 2003, 2004), the spacecraft design and construction industry (Ishimatsu et al., 2010, 2011; Owens et al., 2008; Nakao et al., 2011; Chatzimichailidou et al., 2017; Chen et al., 2015), for missile defense systems, and for railways (Dong, 2012). However, process industry application of STPA is infrequent. Two works among them are the work of Hoel (2012) and Thomas (2013). Hoel (2012) has applied STPA and STAMP to process leaks in the offshore industry. He presented a maintenance control strategy for leak detection and mitigation. An extension of STPA has been proposed by Thomas (2013) for nuclear process system.

In the paper of Abrecht (2016), the author shows the advantages of using STPA compared to traditional techniques. According to the author, STPA can identify all the component failures similar to traditional safety analysis. Moreover, it can find additional safety issues compared to fault tree analysis or FMECA of the system. Pasman (2015) theoretically explains how STPA can replace HAZOP, FMECA, fault tree and event tree analysis. EPRI (Electric Power Research Institute) ran a comparative evaluation of fault trees, event trees, HAZOP, FMECA, and a few other traditional techniques as well as STPA on a real nuclear power plant design. Experts on the methods applied to each hazard analysis technique. STPA was the only one that found a scenario for a real accident that had occurred on that plant design (Fleming et al., 2013).

The work of the present paper is most relevant to the previous work of Rodriguez and Diaz (2016). They have also investigated whether STPA can replace or complement HAZOP in the chemical industry. In their paper, STPA is applied to the lowest level of chemical process and has shown how STPA can be a complement to HAZOP with the help of a case study. They put forward some open questions of using STPA related to the process industry. The questions are how to identify at least one control action for every hazard and how to define system limits from thousands of variables and controllers in the process industry. Further questions are how to choose appropriate states from many states, how to consider many variables and how to cope with the process hazard.

This paper aims to apply STPA (System Theoretic Process Analysis) for Liquefied Natural Gas (LNG) ship-to-ship transfer systems, not investigated earlier. The present article tries to examine some issues mentioned by Rodriguez and Diaz (2016, such as how STPA can consider process hazards like pipe leaks, alarm problems, and others, and how to recognize various process variables considered (pressure, flow, composition, temperature and others). In the paper, the “Methodology” section describes the method of HAZOP and STPA. The “Application” section of HAZOP and STPA presents the case study before the results are presented in the “Results” section and discussed in the “Discussion” section. The final section states the conclusions.

2. Methodology

The present paper describes two hazard identification techniques: HAZOP and STPA. HAZOP is generally used in the planning phase of system development and also in the operational period. STPA uses concepts of system and control theory. It may recognize scenarios which can create a hazard and possibly lead to an accident. STPA tries to identify the measures to eliminate these scenarios by controlling the process.

2.1. HAZOP

The HAZOP technique was initially developed in the 1960s at *ICI* by Kletz and Knowlton to analyze design flaws in chemical process systems. Since then it has been widely accepted and used in the process industries. Other researchers have also developed HAZOP for software (Dunjó et al., 2010; Mcdermid et al., 1995) and computer systems (Glossop et al., 2000; Andow, 1991; Nimmo, 1994; Hulin and Tschachtli, 2011). The method applies to complex processes for which enough design information is available and not likely to change significantly.

2.1.1. Execution of HAZOP

In conducting the analyses, the HAZOP team divides the whole process into segments based on the process P&ID and identifies essential parameters. Each segment is called a node. Some relevant parameters for a process HAZOP can be flow rate (for liquid flow in a pipe), temperature, pressure, liquid level (for liquid storage in a tank). In the next step, guidewords are chosen (see Table 1) and combined with the parameters to create a deviation. For example, when a guideword “no” is chosen for the parameter “flow,” that means the deviation is “no flow” in that node of the system. The team tries to find all possible reasons for and consequences of the deviation and checks whether appropriate safeguards are present to address the deviation and whether there is any need for further improvement. Causes and consequences are sought for other deviations, for example, “high flow,” and “low flow.” The HAZOP team repeats the procedure for other relevant parameters: temperature, pressure, level, composition, vice versa. The team then selects the next node and repeats the whole process.

Table 1 shows a standard set of guide words.

Table 1
Possible guidewords of HAZOP.

Guideword	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN/INSTEAD	Complete substitution

2.2. STPA

The STPA method was developed by Leveson (2011a) to improve the design of sociotechnical systems. The STPA method was developed based on the STAMP (System Theoretical Accident Models and Processes) accident model. According to STAMP, accidents are more than a chain of events. They involve complex dynamic processes and the result of inadequate control actions. This model considers accidents as a control problem, not just a failure problem, and thus, accidents can be prevented by enforcing constraints on component behavior and interactions.

Three crucial elements of an STPA analysis are safety constraints, hierarchical safety control structures, and process models:

- **Safety constraints**: Safety constraints are criteria that must be enforced on the behavior of the system to ensure safety. According to STPA, hazardous control actions or lack of control actions cause hazardous states system of resulting from inadequate enforcement of safety constraints. Safety constraints are controls that should be implemented to ensure the avoidance of hazards, accidental events or accidents.
- **Hierarchical safety control structure**: This diagram presents how systems are viewed as a hierarchy of controllers, enforcing safety constraints between each level. The safety control structure of STPA provides an in-depth means for identifying potentially hazardous control actions, by identifying system behaviors and interactions.
- **Process model**: The process model presents how human operators or controllers' function to control the system. The controller should know the present state of the system to manage it, measures to control and the effect of different control outputs on the network. This statement is true for both automated and human controllers.

2.2.1. Execution of STPA

The STPA method is executed in 5 steps, shown in Fig. 1:

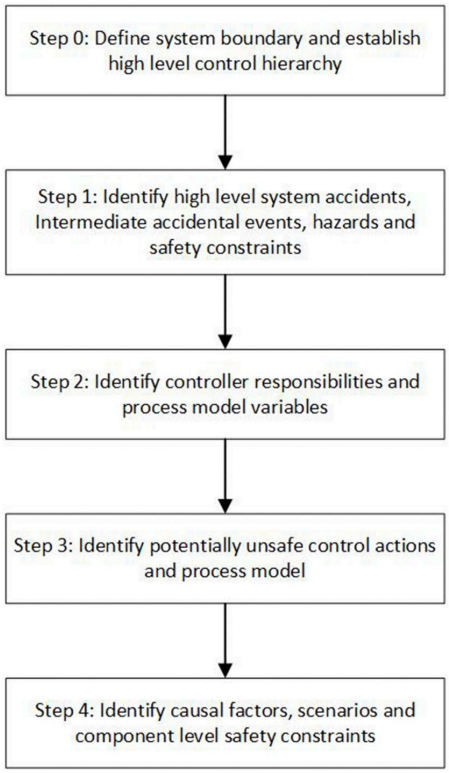


Fig. 1. Workflow of STPA.

Step 1 **Define the system boundary and establish a high-level control hierarchy**:

The first step is to define the scope, which is fundamental to any analysis. This step includes conceptualizing the system as a control system and setting the boundary of the system against other entities.

Step 2 **Identifying high-level system accidents, intermediate accidental events, hazards, and safety constraints**:

This step defines system-level intermediate accidental incidents, accidents, and similar risks. This paper presents system level accidents and hazards as follows:

The terms used in the figure are defined as follows:

Hazard: A system state or set of conditions that, together with a set of operational or environmental conditions, have the potential to lead to an intermediate accidental event or accident.

Intermediate hazardous event: Intermediate failures and combinations of failures or events that initiate from a hazard and that are the cause for the next accidental event to occur.

Intermediate accidental event: An event in a sequence of events that upsets normal operations of the system and may lead to an unwanted accidental incident or accident, may require a response to avoid an undesirable outcome and, if not controlled, may lead to undesired accidental events (Rausand, 2013).

Consequence: Effect of any unwanted or intermediate accidental event.

Accident: An aftereffect of an intermediate accidental event which causes harm to people or environment or asset.

An example of an intermediate accidental event is a leak that may be caused by high pressure or high temperature in a pipeline, high liquid level in a storage tank, external wind or wave, a dropped object or corrosion. So, the hazards are high temperature, high pressure or high liquid level in the system. Uncontrolled hazards may lead to intermediate accidental events (IAE). Uncontrolled IAEs may lead to several consequences and accidents. The leak may lead to accumulation of hazardous material in the process area or dispersion and if ignited may result in fire or explosion or both causing personal injury or fatality or product loss or financial loss. The controller can be an operator or logic controller which can control the hazard, preventing an accidental event from occurring.

Step 3 **Identify controller responsibilities and process model variables**:

It specifies responsibilities and process models for each controller. It influences the next step, where control actions are analyzed. To provide adequate control, the controller must have an accurate model of the process. A process model is used to determine what control actions are necessary to keep the system operating effectively. Accidents in complex systems, particularly those related to software or human controllers, often result from inconsistencies between the model of the process used by the controller and the actual process state (Leveson, 2011). The inconsistency contributes to the controller providing inadequate control. Usually, these models of the controlled system become incorrect due to missing or insufficient feedback and communication channels.

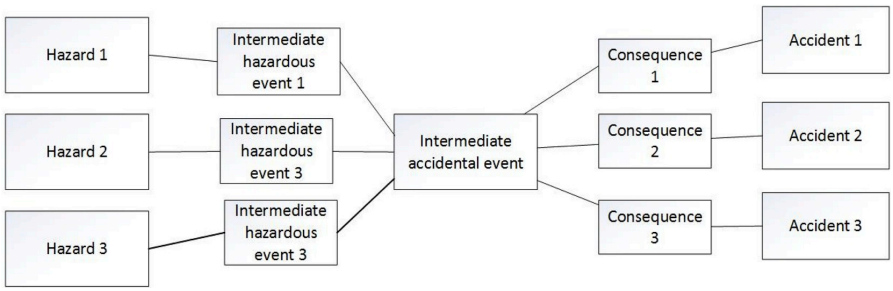


Fig. 2. Hazards, intermediate hazardous events, intermediate accidental events, consequences, and accidents.

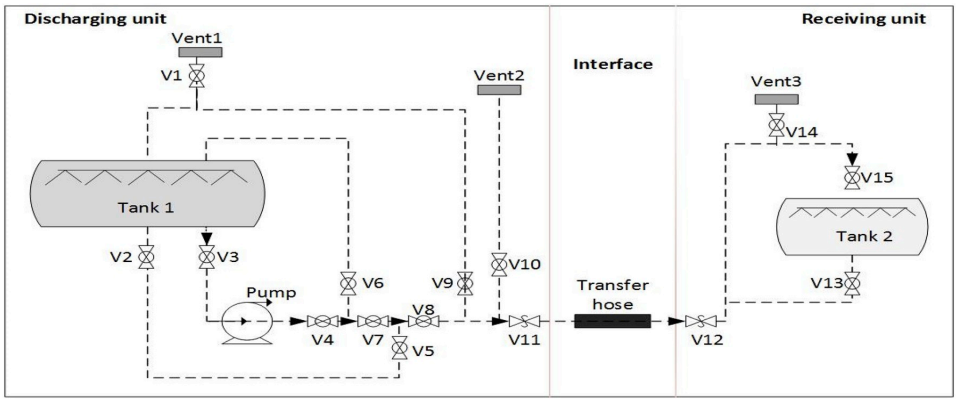


Fig. 3. Process sketch of LNG ship-to-ship transfer procedure.

Step 4 **Identify potentially hazardous control actions and process models**:

Identifies the potential for inadequate control of the system that can lead to a dangerous state. According to Leveson (2011), hazardous states result from inadequate controls or enforcement of safety constraints, which can occur because:

1. A control action required for safety is not provided, or not followed
2. A hazardous control action is provided
3. A potentially safe control action is provided too early or too late, or in the wrong sequence
4. A control action required for safety is stopped too soon or applied too long

A control action by itself does not provide enough information to determine whether it is safe or hazardous. Additional information is necessary, including the context of the environment. Considering each responsibility of each controller can identify potential hazardous control actions for a system.

Step 5 **Identify causal factors, scenarios, and component-level safety constraints**:

Determine how each of the hazardous control actions could occur by identifying causal factors and scenarios. This goal is achieved by investigating each element of the control loop or control hierarchy and assessing whether any of the elements could cause hazardous control actions in question. After identification of scenarios and causal factors, one can identify safety constraints. Safety constraints keep the system from hazardous states or mitigate the consequences.

3. Application of HAZOP and STPA to STS transfer of LNG

In this section, HAZOP and STPA have been applied to the LNG STS (ship-to-ship) transfer system. The intention is to demonstrate how hazard analysis can be accomplished for the system, using the two methods. The considered system is as generic as possible.

LNG STS transfer for marine systems is the transfer of LNG from or to an LNG carrier vessel (LNGC) to or from an LNG storage ship or floating storage and regasification unit (FSRU). With the increasing demand for energy, LNG ship-to-ship transfer has increased to supply low cost liquefied natural gas to remote areas where local energy resources are scarce. The transfer is done using high-pressure pumps. The consequences of loss of containment during this operation can be severe. The traditional method of risk analysis for these types of systems is HAZOP (Crawley and Tyler, 2000), where the objective is to improve the design to establish a safe design.

3.1. System description

STS transfer of LNG is carried out in port. After arrival and mooring of an LNG cargo ship, required tasks include inserting the LNG transfer line, checking storage tank systems and related equipment, earthing, connecting hoses & links, opening the manual and automatic valves and, finally, starting the pump. After completion of the liquid transfer, operators stop the pump, purge the lines, and disconnect the hoses. It is essential to follow the sequence to ensure the safe and proper execution of the transfer.

The main component of the STS transfer process is the pump. Other vital components include control valves, motors, hoses, and pipelines. During operation, flexible pipes from the storage tank of the carrier ship are connected to the storage tanks of the storage ship by manifold.

Table 2
HAZOP for LNG transfer (part of).

Parameter	Deviation	Causal factors	Consequences (system reaction)	Actions required
Flowrate	1.1 High	Ship pump malfunction, control valve malfunction, PLC failure, undefined procedure, boundary conditions, threshold value, valve fully open due to debris, debris suddenly loosened	High level in the tank, High flow over a period may cause flow-induced vibration, may cause pipe rupture and leakage	Consider flow meter and high-level alarm if not previously identified, clarify design basis
Pressure	2.1 High	PCV failure, an inadequate volume of vents, external fire, weather condition, changes in density, external fire	Fire, explosion, fluid loss, water hammer on site, rupture of the pipe	Assess risk and redesign pressure protection system Adjust PSV set points, implement new shut down functions, improve the reliability of shut-down functions, improve the operational procedure
Temperature	3.1 high	The ambient condition, fire situation, defective control valve, internal fire, faulty instrumentation and control, cooling system failure, mechanical heating	LNG loss via a relief valve	Improve the reliability of thermal valves
Composition	4 Abnormal contamination	Bad LNG quality from ship, leaking isolation valves, incorrect operation of the system, ingress of air, ingress of water, corrosion, gas entrainment	LNG inside tank polluted, corrosion or erosion inside the pipe	Check design basis against operational experience
Concentration	5 Low	Impure raw material, leak in the line, phase change, process control upset, gas entrainment	Performance of equipment gets affected, contaminated product, chances of severe working conditions	Check material quality
Level	6.1 high	The ship does not stop unloading (operator mistake or pump malfunction), outlet isolated or blocked, faulty level measurement, corrosion, pressure surge, Wrong level information (sensor problem), leakage on the storage tank	Fluid leakage on PRV due to a pressure increase	Install reliable level sensor Take protection for corrosion, blockage
Service failure	7	Electric power, water supply, telecommunications, PLCs/computers, HVAC, fire protection, steam	Abort of operation	Check for an alternative arrangement of electricity, water.

Motors can control the speed of the pumps, and valves are used to control or regulate the flow of liquid. Thermal relief valves are installed with pipes to control the temperature or pressure of the fluid. Emergency relief valves or emergency relief couplings are connected to stop the liquid transfer or disconnect the pipe during an emergency. The pump creates a pressure difference between both ends of the pipeline to establish the desired flow. The function of the electrical system is to provide energy to operate the motor driving the pump. Thermal relief valves are installed to reduce pressure or temperature effects on the network. These can be controlled automatically or manually. For the actuators to perform the commands, an adequate amount of power must be available. In this analysis, we do not specify any power system solution to keep the study generic (see Fig. 2).

Advanced process systems are equipped with logic controllers or programmable controllers, by which all the components, like pumps and valves, can be controlled. Control room operators can observe all operations of the plant to ensure everything is working correctly. Fig. 3 presents a simplified process flow diagram. It is common practice to apply a top filling, to reduce the pressure in Tank 2. Excessive pressure may make the pumps work harder. Transfer speed ranges from 100 to 1000 m^3/hr, depending on the scenario, tanks, and equipment. This rate can be altered during transfer to reach a pre-established amount. Both ship authorities can monitor conditions of the transfer, e.g., system pressure, tank volume, and equipment behavior. To start the transfer from *Tank 1* to *Tank 2*, *valves V3, V4, V7, V8, V11, V12, and V15* must be opened.

3.2. Execution of HAZOP

Before the execution of HAZOP, HAZOP team specifies the specific nodes from the P&ID. Control lines are in dotted line in Fig. 3. Arrow lines show the route of liquid flow. The team chooses one node first. Next, they search for appropriate parameters and guide words. The present case uses parameters like flow rate, pressure, temperature, composition, and liquid level. It also uses additional parameters related to operational safety, (e.g., service failure, maintenance, abnormal operation, information). Guidewords chosen are “High,” “Low,” “No,” “Reverse” and others. The team searches for possible causes and consequences for each deviation. For example, what are the causes of “High temperature,” and what might be the consequences? Recommendations are made to avoid the deviation “High temperature” and the possible consequences of the deviation. Table 2 shows part of HAZOP worksheet.

3.3. Execution of STPA

3.3.1. Define system boundaries and establish a high-level control hierarchy (step 0)

This step defines the STS system boundaries and establishes a high-level control hierarchy. Fig. 4 shows the high-level control structure of an STS transfer system. The system consists of three controllers, actuator systems and disturbance processes (wind, waves and current). Three kinds of controllers are logic controllers (also called auto controllers), control room operators and site operators. The objectives of the controllers are to induce the desired flow of liquid in the pipeline by providing suitable commands to actuators and to protect the system from external disturbances. Actuators and disturbances affect the STS process. The control hierarchy diagram (Fig. 4) provides the means to communicate between developers, analysts, and users. It also includes other relevant information.

The logic controller (or programmable controller) is a digital computer which can control the process equipment such as the speed of pumps and motors, opening or closing process or safety valves, vice versa. Control room operators can control some equipment or states of the system. For example, the flow of electricity and the opening or closing of valves by getting feedback from the sensors attached to the

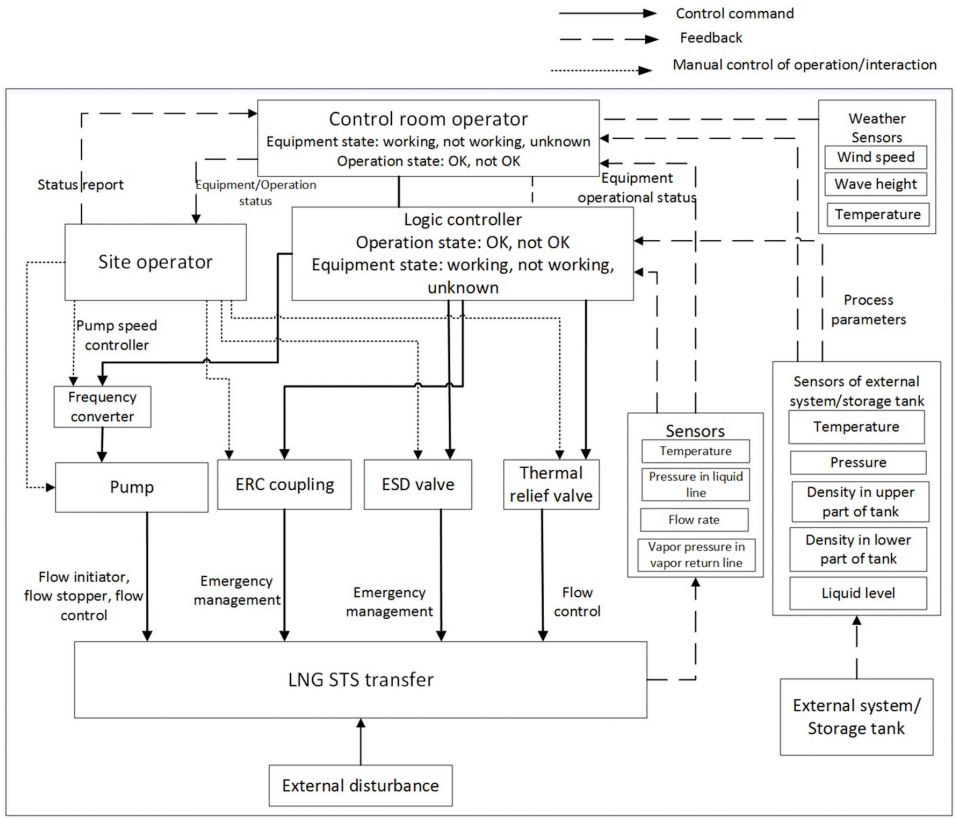


Fig. 4. High-level control diagram of LNG STS transfer.

system. In process systems, the site operator has an important role. He (or they) monitors the plant during a site visit and takes appropriate actions. In cases where the automatic controller cannot act, or the control room operators cannot fix the problem, they are responsible for setting the problem manually since they are physically present.

The actuation system is composed of pumps, non-safety valves, thermal relief valves, emergency relief coupling, and emergency shutdown valves (see Fig. 3). For automatic control, they get commands from logic devices to go into the position of "open" or "closed" to relieve thermal energy into the environment. The logic device determines this requirement from the feedback of sensors. Here, we consider each component not only as a component of the system but also as an actuator of the system which can control the operation.

3.3.2. Identification of system-level hazards, accidents, intermediate accidental events and safety constraints (step 1)

To keep the system safe, we want to avoid system-level accidents and unwanted intermediate accidental events. First, we define system level accidents and adverse intermediate accidental events and their related hazards. There can be many unexpected events which lead to an accident. From the *Hazards and Accidents List,* we define safety constraints to avoid them. " One important aspect of the analysis is to follow the control objectives. Control objectives depend on the function of the system in the operational context. In this case, the control objective is to make the liquid flow within the defined limit. Accidents or hazards may occur if control objectives are not followed or are not suitable for the operational function of the system. System-level safety constraints can be derived directly from the hazards and should include constraints to *avoid* accidents. For the present case, one accidental event is "Leak in System". Table 3 summarises system-level safety constraints related to leakage in the system.

3.3.3. Identification of process model variables and controller responsibilities (step 2)

This step defines process model variables from the high-level safety constraints. Process model variables are those parameters in a system that needs controller action to keep the system operating safely. Process model variables can identify controller responsibilities. Different responsibilities of each controller in the control hierarchy need to be defined to identify hazardous control actions. In STPA, each responsibility, or each specific control action derived from the responsibilities, is considered concerning whether it can cause weak enforcement of safety constraints. Table 3 shows process model variables for each high-level system hazards and accidents.

3.3.4. Identifying hazardous control actions and process model for the control actions (step 3)

In this step, we use the control actions and process model variables to identify hazardous control actions. Table 4 presents the hazardous control actions identified for an unexpected event of leakage in the system. Analysts identify hazardous control actions by considering each generic mode of unsafe control and relevant process model variables. Later, we establish the process model to determine the circumstances requiring hazardous control action. From the process model, we can see controller actions, responsibilities, and entities giving feedback to controllers and actuators involved to execute one single control action.

Table 3
High-level system hazards, safety constraints, process model variables and possible control actions in the process for each intermediate accidental event (part of).

Intermediate accidental event: 'Leak.'			
High-level System hazards	High-level Safety constraint	Process model variables	Examples of control actions
H1: High pressure in the system	The pressure in the system should not exceed a defined limit The temperature in the system should not exceed a specified limit A fire that occurred nearby should not affect the system	High pressure in the system A high temperature in the system	Activate pressure relief valve Activate process safety valve Extinguish fire Check insulation on the pipeline
H2: Low pressure in the system	The pressure in the system should not be below a defined limit	Low pressure in the system Pump speed	Check pressure control valve Check vent valve Regulate pump speed as desired Check for a leak in the system Protect system against leakage
H3: High temperature in the system	The temperature should not exceed a defined limit The pressure in the system should not exceed a specified limit A fire that occurred nearby should not affect the system	A high temperature in the system High pressure in the system	Activate pressure relief valve Protect the system from sunlight Extinguish fire Check insulation on the pipeline
H4: Low temperature in the system	The temperature in the system should not be below a defined limit	Low temperature in the system Low pressure in the system	Check for a leak in the system Check pipeline insulation
H5: Liquid level exceeds the high limit of the storage tank	The liquid level should not exceed a defined limit	Liquid level high	Stop the pump
H6: High flow rate in the pipe	Flowrate should not exceed a specified limit	High flow rate	Control flowrate Check pump functionality Check valve functionality Check the pipe network for debris
H7: Low flow rate in the pipe	Flowrate should not be below the defined limit	Low flowrate	Control flowrate Check pump functionality Regulate pump speed as desired Check valve functionality Check the pipe network for debris Check pipe network for leak

In this case, one hazard is high pressure in the pipe system, which can be reduced by opening a pressure relief valve. The control action here is "Activate Pressure Relief Valve". A logic controller or a control room operator or a site operator can execute the action. A pressure sensor attached to the pipe system gives feedback to the logic controller, which is visible to the control room operator also. The site operator can see the sensors physically. Table 4 presents hazardous control actions. The process model helps to identify causal factors and scenarios. Fig. 5 shows an example of a process model, how a pressure relief valve works to control the process. The sensor gives feedback to the logic controller when there is high pressure in the system. The logic controller can give the command "open" or "close" to pressure relief valve to relieve pressure. The control room operator can be aware of the state of operation and can give a command to the logic controller to act or can inform the site operator to take action when the logic controller cannot control the system automatically.

3.3.5. Identifying causal factors and scenarios (step 4)

After identifying hazardous control actions in the previous step, this step identifies potential causes and their preventive measures. Accidents can occur by any action which is not hazardous directly but creates a hazardous situation. For example, if controllers provide appropriate safe action, but in the wrong order or using the wrong procedure, it may lead to an accidental event or accident. Overall, the step tries to identify violations of safety constraints or how they can occur (scenarios). Scenarios can be determined to enhance knowledge about why and how hazardous control actions can happen, and associated causal factors. Table 5 presents causal factors for hazardous control actions.

4. Discussion

This paper makes a comparison between two hazard identification processes, HAZOP and STPA. LNG STS transfer process has been chosen to investigate the feasibility of the application of STPA for a modern process plant that requires human intervention to a large extent, which is a characteristic of a sociotechnical system. Table 6 presents a comparative analysis. The analysis of the present case study shows the effectiveness of STPA as declared.

To conclude that STPA can replace HAZOP, it must cover all the functions of HAZOP. To say that STPA can be complementary to HAZOP, it should provide an improved risk picture if performed. It should demonstrate the issues which are not covered by HAZOP but can be covered by STPA. The authors of the present paper classified the identified hazards from the analyses into the following five error categories:

- Human and organizational errors
- Software errors
- Component errors
- System errors
- External events

The two methods are compared based on these error categories. Other qualitative criteria are discussed later, i.e., documentation requirements, time requirements, resource requirements, level of detail, confidence in results and applicability.

4.1. Human and organizational errors

The case study results show that STPA can cover more organizational errors. The results are almost the same for both cases in the identification of human errors. Human HAZOP or human factors (HF) HAZOP are being used nowadays to analyze human interaction or involvement. Different guidewords are used then such as 'no action taken,' 'action was taken later,' 'more action was taken' to conduct human HAZOP. The present case study performs a traditional HAZOP and makes a comparison with STPA based on that. The parameters used in the case study are identical to those used in the conventional HAZOP. It is challenging to identify organizational deficiencies in a HAZOP

Table 4
Hazardous control actions (part of).

No	Control action/event	Control action not provided causes hazard	Control action provided when not required causes hazard	Control action provided too early causes hazard	Control action provided too late causes hazard	Control action stopped too soon or applied too long
1	Open PRV	PRV valve is not activated when pressure/temperature exceeds the high limit	PRV opened when pressure/temperature is within range	N/A	PRV/PSV is opened too late after detection of high pressure/temperature	N/A
2	Mitigate fire	The fire protection system is not activated when there is fire	The fire protection system is activated when there is no fire	N/A	The fire protection system is activated too late when there is fire	Fire protection system gets off before the fire is mitigated
3	Check insulation on the pipeline	Missing pipeline insulation check and insulation protection is absent	N/A	N/A	N/A	N/A
4	Check valves functionality	Regular maintenance check on the valves is missing	N/A	N/A	N/A	N/A
5	Regulate pump speed as desired	Pump speed cannot be regulated as desired	N/A	N/A	N/A	N/A
6	Check for a leak in the system	Check for leakage in the system is missing	N/A	N/A	N/A	N/A
7	Protect system against leak	Leak protection measures are missing	N/A	N/A	N/A	N/A
8	Protect the system from sunlight	The sunlight protection system is absent	N/A	N/A	N/A	N/A
9	Control flowrate	Controllers cannot control the flow rate when the flow is not within range	N/A	N/A	The flow rate is controlled too late when the flow is not within range	N/A

compared to STPA. The reason for this is that HAZOP was developed to find deviations caused by the system in the process industry, not to find deviations in human action or organization. STPA uses a hierarchical control diagram to show the whole system along with its interaction with other components, and their effects on the network. As it uses a systematic process to identify safety constraints, organizational deficiencies and requirements can be included, something which is not possible in traditional HAZOP. Moreover, the control hierarchy established in the paper for STPA does not cover much of the organization "above" the operation. The extended structure can find more deficiencies.

4.2. Software error

Identification of software error requires a good understanding of software behavior, interactions and effects on other systems. HAZOP is less efficient in the treatment of software error because both hazardous and non-hazardous data flows must be analyzed. The presence of complicated software limits the use of classical techniques. By applying a combination of traditional HAZOP, HF HAZOP and Software HAZOP, more hazards could have been identified, but this requires further work.

4.3. Component error

The results are almost the same for identifying component errors. HAZOP has proven to be a useful tool for identifying and evaluating component-related hazards associated with the processes utilized in the hydrocarbon and chemical industries. The fact that STPA produces very similar results indicates that this method is equally valid. HAZOP is considered suitable for identifying hazards arising from single, independent contingencies.

4.4. System error

HAZOP can identify any deviation in the system quickly. We do not explicitly mention the environmental conditions of execution. System safety is built into the design to ensure that, for each deviation in a process parameter, at least two levels of safeguards protecting against deviation and operator actions are included (Goyal, 1993). In STPA, success, however, depends on proper identification of intermediate accidental events. Low-level hazards which do not belong in the class of any accidental events and hazardous control actions may have fallen outside the scope of analysis. We should include actors, preconditions, alternative flows and non-functional requirements in the study to mitigate for this.

4.5. External events

In STPA, using the control hierarchy diagram, the effects of external events can be identified conclusively in a systematic way. HAZOP is also able to determine the outcomes. However external events are traced in an unsystematic way, which gives an uncertainty of the completeness of the analysis to consider all the event.

4.6. Documentation requirements

HAZOP is performed based on the process flow diagram (PFD) or P& ID, developed at the design stage. STPA examines the essential functions of each entity in the control loop and the requirement for effective safety system behaviors. One can redefine goals and related system performance and may develop alternatives for analysis. This approach emphasizes the importance of the process model in enforcing adequate control. System behavior is expressed in relationships that represent the structure of the system in a hierarchical control model. One can work with STPA with a primary process flow diagram (PFD) before establishing the detailed process and instrumentation diagram (P&ID).

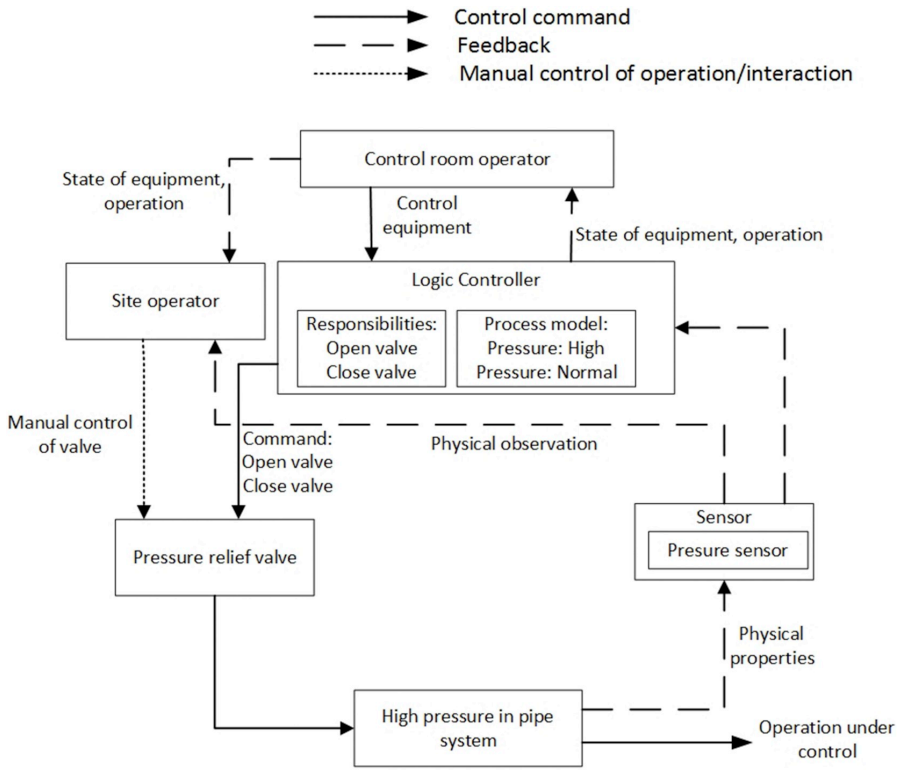


Fig. 5. Process model to control pressure in LNG transfer system.

4.7. Time requirements

This criterion relates to how time-consuming the methods are to apply to a specific application. The industry is using HAZOP for a long time. Industry personnel is well known in the method and execution process. The method is also straightforward, and those not familiar with it usually understand it very quickly.

On the other hand, STPA is quite a new method, especially have not implemented for the process industry applications. Industry personnel may find it challenging to execute. Identification of causal factors and step-by-step execution can be challenging. Including the system study, the analysis time required for STPA was three times longer than the time needed for HAZOP for this study. This negative aspect of STPA may indicate that it should be used not necessarily for complete process systems but for more limited parts of the system, which are particularly challenging to analyze with HAZOP.

4.8. Resource requirements

To conduct a HAZOP, experts from all disciplines need to participate face to face and check the deviation. Feedback from all discipline experts is considered to find the deviation, e.g., electrical, automation, instrumentation, software, process. Resource requirement is the same in the case of STPA.

4.9. Level of details

HAZOP follows a deductive or downward approach like top events and deviations and tries to find what would happen to the system due to the deviation. This approach is easy to follow and has made HAZOP widely accepted for the analysis of systems (Hoepffner, 1989). However, this type of analysis becomes difficult when the boundaries of the study are too vast, and guidewords become too numerous. There is no systematic method to limit the guide words. HAZOP identifies causes of deviations but does not usually go into detail analysis of causes. STPA, in general, can go into details in deriving causes of failures in a better way. Its step-by-step and systematic approach assures identification of all potential hazards. Users can refine every hazard and safety constraint at the lower level and can go into the details of each issue of system requirements. However, for process industry applications, to set the boundaries of study, to find the required number of variables to be studied, the necessary control actions for each safety constraint, and the role of controllers for each control action needed (CA) in STPA are also challenging. The process industry uses thousands of variables, and they can be in various states (online, offline, in maintenance).

4.10. Confidence in results

The confidence of decision-makers in the analysis and its effects are an important factor in decision-making. In this respect, HAZOP has an advantage since it is a popular method that has been shown to work for decades, while STPA is quite a new method. Risk assessment may help people evaluate the risks they face. Information is needed to identify those risks to take precautionary measures. People have more confidence in studies that are in line with prior beliefs. In the case of a new method, the user may not find the confidence to use it, even if it is superior. In STPA, the user may get confidence from its level of detail. However, the success depends mainly on the proper establishment of a functional control diagram. A disorganized functional control diagram may lead to an incomplete result and completely unuseful analysis. On

Table 5
Causal factors and low-level safety constraints for each hazardous control actions (part of).

Hazardous control actions	Causal factors	Low-level safety constraints
Controllers cannot activate the pressure relief valves when pressure/temperature exceeds the high limit	1 Pressure sensor failure 2 Pressure relief valve failure 3 Communication error 4 Auto-activation is turned off 5 The problem in decision-making arrangement. 6 Electricity blackout 7 The operator is reluctant to act due to high workload 8 Poor audibility/visibility of sensor 9 The operator is confused to follow the procedures	1.1 Sensors must be designed to operate for X years with no defect 1.2 There should be a maintenance program to test the sensors after Y year, to replace after Z years 2 There should be a check of valves after every Y year 3 Good communication arrangement between control room operators and site operators 4 Mode of each system/component should be defined clearly 4.1 The operator should know in which mode each component is working 4.2 The operator should know the exact control actions to be performed by auto controllers or not 4.3 Operators should know the timeframe within which auto controllers need to activate and maximum allocated time until controllers take action 5 Alternate energy source should be available 6 Operator's maximum working time should e followed according to regulation 7 The maintenance program should be established to check the audibility/visibility of sensors before starting operation 8 Should be trained for operating each component and valve manually
The pressure relief valve is activated when pressure is within range	1 Pressure sensor malfunction 2 Communication error	Mentioned earlier
Fire suppression system is not activated when a fire is detected	1 Detector malfunction 2 Communication error (missing signal) 3 The operator is reluctant to act due to high workload 4 Poor audibility of the detector 5 The operator is confused about the procedures	Mentioned earlier
Fire suppression system is activated when there is no fire	1 Detector malfunction 2 Communication error	Mentioned earlier
Missing pipeline insulation check and insulation protection	1 The job is out of scope in the maintenance log 2 The operator is reluctant to perform the task 3 Lack of operator training	1 Update maintenance log regularly 2 Follow the standard working time of an operator 3 Provide adequate training and trainer to operators 4 Provide well-insulated pipe

the other hand, a well-organized functional control diagram is the most significant strength of STPA.

4.11. Applicability in a specific application

The last criterion is to assess how applicable the analysis is to identify different types of hazards in various industry. From the comparative analysis (Table 6), STPA is shown to be more capable of identifying organizational error and the effects of external events. The case study chosen here is for a simple system. The result became very similar in the case of the two analyses. Possibly, results may become significantly different for a more complex system. STPA would be more suitable to apply for a complex system as it tries to find the hazards in a very systematic way. The challenge of STPA would be to deal with many variables and controllers, the number of state variables, the number of variables and above all defining the system limit (Rodriguez and Diaz, 2016).

Moreover, for complex systems, the time required to conduct STPA may become very long compared to HAZOP. That is a significant disadvantage of STPA. However, the longer time can be justified as STPA provides a more detailed analysis and takes a short time for future modification of the plant.

The findings of the paper confirm the results of the article by Rodriguez and Diaz (2016) that the differences between both techniques are not very important at the lowest level. The advantage of using STPA is that the analysis is very systematic and very suitable to apply for a sociotechnical system. STPA requires one single study to be conducted to cover all aspects of errors. One can readily design the mitigation strategy and can evaluate their effectiveness from control algorithms through scenario analysis. STPA can capture the dynamic behavior of systems. The root scenario can be used to communicate the need for mitigation strategies at board levels. The control diagram describes the faulty or malicious system behavior at a high level and points out the potential system losses.

Industry uses a combined approach, HAZOP for hazard identification and SIL (Safety Integrity Level) for risk analysis. They use other assessments on a case-by-case basis, e.g., human factor, system reliability, CHAZOP. CHazop can be overwhelming when performed on a complex software system with large quantities and varieties of data flow. In the case of a process-oriented control system with very little flow of information but with a complicated control algorithm, the data flow may not be the right unit of analysis (Thomas, 2013). HAZOP relies on the user's understanding of software behavior, interactions and effects on other systems.

Compared to a traditional human factor model, in STPA, scenarios and causal influences are easy to identify using the human controller model as a starting point. It can address issues related to human-automation interaction before the final automation design finalized. The role of the human operator on system operations can be analyzed, and design can be modified accordingly. Unlike the automated controller, the human has a control-action generator rather than a fixed control algorithm. One advantage of having a human in the loop is the flexibility to change procedures or create new ones in a situation.

5. Conclusion and future work

The objective of this article has been to assess the feasibility of using STPA for hazard identification in automated process systems and determine whether STPA can replace traditional HAZOP or become complementary to HAZOP. A specific process system, a ship-to-ship transfer system for LNG is used to perform the analyses and to make the comparisons. The study shows that the causes identified by STPA and HAZOP are almost identical. Possible causes identified by STPA cover hardware failures and communication errors, including delayed

Table 6
Comparison between HAZOP and STPA (part of).

Hazard category	Identified by HAZOP? Examples	Identified by STPA? Examples
Component error	Ship pump malfunction	Ship pump malfunction
	Sensor malfunction	Pressure or level sensor malfunction in functionality, audibility or visibility
	PRV/control valve/check valve failure	Detector failure
	Logic control failure	Control equipment malfunction
	Vent valve open	Emergency rescue equipment malfunction
	Low audibility/visibility of sensor	Fire suppression system malfunction
Organizational error	Operators did not follow the unloading procedure mentioned in the protocol	An alternate system is not available during maintenance due to lack of redundancy or planning
	Ignorance about operational boundary (Flow, Pressure, Temperature)	The organization does not follow a standard working time of operators
		Lack of a healthy working environment
	Ignorance about the operational condition (empty tank, pressure, temperature, level)	Lack of a well-documented operational procedure
		Insufficient preparation before the operation
		Lack of well-trained resource, Lack of training about equipment handling, emergency rescue action, corrosion check, leak check
		Lack of communication between interdisciplinary team
		Lack of satisfaction of workers about workplace, salary or facility provided
		Wrong decision making by managers in the operational procedure
		Missing regular update of maintenance log, Low reliability of equipment or instruments
		Insufficient redundancy of equipment
		Poor planning of the operation, Lack of existence or implementation of accident prevention strategy (high wave, wind, ignition, dropped object)
		Lack of operators' safety procedures
Human error	Valve half closed/entirely closed during operation	Operator not aware of the operating condition or system condition or instrumentation malfunction or product quality
	Bad LNG composition, Debris in the pipeline	Missing action of the operator due to high workload or dissatisfaction about work
	External Water/particles inside the product	Wrong operation of an operator
	Remaining pressure in line	Wrong operational procedure
	The operator gives the wrong command	The late arrival of the emergency rescue team
	More injection of wax/scale inhibitor	Maintenance log is not updated regularly
	Wrong operational procedure	Poor insulation of pipe or product quality check
	Incorrect information about pressure, temp, level	
Software error	Valve half closed/entirely closed during operation	Wrong voting arrangement
		Bug in software, Intentional sabotage or hacking of software
System or design error	Electricity blackout	Electricity blackout, Communication error
	Leakage in pipeline	Leakage in pipeline
	Internal leakage in valves	Overpressure/overheating of equipment
	Overpressure/overheating due to fire/PRV failure	Insulation failure
	Insulation failure	Missing emergency rescue action
	Liquid accumulation in line, Remaining pressure in line	Poor or missing insulation of pipe
	An unwanted shutdown of the system	The system is not protected against the high wave, wind or dropped object
	Missing emergency rescue action, Flow-induced vibration	Logic control system malfunction
	Local instrument missing	
External events		The system gets affected by wind, wave or dropped object.

communication and software errors, which is the case for HAZOP also.

The results show that STPA is a systematic hazard analysis technique that provides systematic guidance and recommendations for safety requirements. The primary challenge in STPA is to establish the control structure. However, the process of developing the control structure is a beneficial process because it provides additional insight into how the system works, in particular, on the higher level of the hierarchy. For complex systems which involve highly automated systems and many interactions of components, STPA can be applied to understand the system's behavior. It ensures the completeness of the hazard list and can link different control structure diagrams from a high level to a detail level. For any process system that involves simple interactions and less software, HAZOP can be more suitable, considering its simplicity and lower time requirement. Authors draw a conclusion based on the present case study. Other additional case studies may provide further perspectives on the use of the method.

The present paper tries to solve some questions raised earlier (Rodriguez and Diaz, 2016), such as how STPA can consider process hazards like pipe leaks, alarm problems, and how the process variables can be considered (pressure, flow, composition, temperature, and others). Some questions still need to be solved like how to define system limits among thousands of variables and controllers. Future studies can be conducted on other process industry applications to identify workflows of multiple controllers and determine timing and sequencing of each control action, to reduce elapsed time between each step and introduce more sophistication in the process.

Acknowledgments

The project is financed by *DynSoL AS and Research Council*, Norway, through research project number 283861 and performed at the *Department of Marine Technology, NTNU*. The authors of the paper wish to thank Professor Ingrid Bouwer Utne at the *Department of Marine Technology, NTNU*, for sharing her knowledge in system safety engineering and risk assessment; Børge Rokseth, Researcher at *Marine Technology Department, NTNU,* for sharing his experience of working with STPA on DP systems. We are thankful to Dr. A F M Kamrul Islam, Project Manager of DynSoL AS research project for his valuable support in HAZOP assessment.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.jlp.2019.04.005.

8 References

Abdulkhaleq, A., Lammering, D., Wagner, S., Roder, J., Balbierer, N., Ramsauer, L., et al., 2017. A systematic approach based on STPA for developing a dependable architecture for fully automated driving vehicles. In: 4th European Stamp Workshop 2016,

Esw 2016. vol 179. pp. 41–51.
Abdulkhaleq, A., Wagner, S., Leveson, N., 2015. A comprehensive safety engineering approach for software-intensive systems based on STPA. In: Proceedings of the 3rd European Stamp Workshop. 128. pp. 2–11.
Abrecht, B.R., 2016. Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System. Massachusetts Institute of Technology.
AMES Research, C., 1973. Failure Mode, Effects, and Criticality Analysis, Moffett Field, Calif. National Aeronautics and Space Administration.
Andow, P., 1991. Guidance on HAZOP Procedures for Computer-Controlled Plants. Health and Safety Executive, Great Britain.
Barlow, R.E., Chatterjee, P., 1973. Introduction to Fault Tree Analysis. California Univ Berkeley Operations Research Center.
Chatzimichailidou, M.M., Karanikas, N., Plioutsias, A., 2017. Application of STPA on small drone operations: a benchmarking approach. In: 4th European Stamp Workshop 2016, Esw 2016. 179. pp. 13–22.
Chen, J.Y., Lu, Y., Zhang, S.G., Tang, P., 2015. STPA-based hazard analysis of a complex UAV system in take-off. In: 3rd International Conference on Transportation Information and Safety (Ictis 2015), pp. 774–779.
Crawley, F., Tyler, B., 2000. HAZOP: Guidelines to Best Practice for the Process and Chemical Industries.
Dong, A., 2012. Application of CAST and STPA to Railroad Safety in China. Massachusetts Institute of Technology.
Drogoul, F., Roelen, A., Kinnersly, S., 2005. Towards an approach to building safety into design. Science 42.
Dunjó, J., Fthenakis, V., Vílchez, J.A., Arnaldos, J., 2010. Hazard and operability (HAZOP) analysis. A literature review. J. Hazard Mater. 173, 19–32.
Eargle, L.A., Esmail, A., 2012. Black Beaches and Bayous: the BP Deepwater Horizon Oil Spill Disaster. University Press of America, Inc.
Fleming, C., Placke, M., Leveson, N., 2013. Technical Report: STPA Analysis of NextGen Interval Management Components: Ground Interval Management (GIM) and Flight Decn Interval Management (FIM). MIT.
Glossop, M., Loannides, A., Gould, J., 2000. Review of Hazard Identification Techniques. Health & Safety Laboratory.
Goyal, R., 1993. Hazops in industry. Prof. Saf. 38, 34.
Hoel, F., 2012. Modeling Process Leaks Offshore Using STAMP and STPA. Institutt for Produksjons-Og Kvalitetsteknikk.
Hoepffner, L., 1989. Analysis of the HAZOP study and comparison with similar safety analysis systems. Gas Sep. Purif. 3, 148–151.
Hulin, B., Tschachtli, R., 2011. Identifying software hazards with a modified CHAZOP. In: PESARO 2011 First Int. Conf. Performance, Saf. Robustness Complex Syst. Appl. 12. pp. 7.
Ishimatsu, T., Leveson, N., Fleming, C., Katahira, M., Miyamoto, Y., Nakao, H., 2011. Multiple controller contributions to hazards. In: 5th IAASS Conference, Versailles, France.
Ishimatsu, T., Leveson, N., Thomas, J., Katahira, M., Miyamoto, Y., Nakao, H., 2010. Modeling and Hazard Analysis Using STPA.
Khan, F.I., Abbasi, S.A., 1999. Major accidents in process industries and an analysis of causes and consequences. J. Loss Prev. Process. Ind. 12, 361–378.
Kletz, T., 1995. Some Incidents that Have Occurred, Mainly in Computer-Controlled Process Plants. Computer Control and Human Error.
Leveson, N., 2011a. Engineering a Safer World: Systems Thinking Applied to Safety. MIT press.
Leveson Nancy, G., 2011. STPA: A New Hazard Analysis Technique. MIT Press.
Leveson, N.G., 2003. A new approach to hazard analysis for complex systems. In: International Conference of the System Safety Society.
Leveson, N.G., 2004. Model-based Analysis of Socio-Technical Risk.
Leveson, N.G., 2011b. Applying systems thinking to analyze and learn from events. Saf. Sci. 49, 55–64.
Marais, K., Dulac, N., Leveson, N., 2004. Beyond normal accidents and high-reliability organizations: the need for an alternative approach to safety in complex systems. In: Engineering Systems Division Symposium, pp. 1–16.
Mayer, G., Zubir, W.A., Ming, L.A., Chang, R., 2003. Tele-maintenance for remote online diagnostic and evaluation of problems at offshore facilities, sarawak. In: SPE Asia Pacific Oil and Gas Conference and Exhibition. Society of Petroleum Engineers.
Mcdermid, J.A., Nicholson, M., Pumfrey, D.J., Fenelon, P., 1995. Experience with the application of HAZOP to computer-based systems Computer Assurance. In: COMPASS'95. Systems Integrity, Software Safety, and Process Security. Proceedings of the Tenth Annual Conference on, 1995. IEEE, pp. 37–48.
Nakao, H., Katahira, M., Miyamoto, Y., Leveson, N., 2011. Safety guided design of crew return vehicle in concept design phase using STAMP/STPA. In: Proc. Of the 5: the IAASS Conference, pp. 497–501 Citeseer.
Nimmo, I., 1994. Extend HAZOP to computer control systems. Chem. Eng. Prog. 90, 32–44.
Othman, N.A., Jabar, J., Murad, M.A., Kamarudin, M.F., 2014. Factors influencing safety management systems in petrochemical processing plants. J. Technol. Manag. Technopreneursh. 2.
Ouddai, R., Chabane, H., Boughaba, A., Frah, M., 2012. The Skikda LNG accident: losses, lessons learned and safety climate assessment. Int. J. Glob. Energy Issues 35, 518–533.
Owens, B.D., Herring, M.S., Dulac, N., Leveson, N.G., Ingham, M.D., Weiss, K.A., 2008. Application of a safety-driven design methodology to an outer planet exploration mission. In: Aerospace Conference, 2008 IEEE. 1–24 IEEE.
Paltrinieri, N., Tugnoli, A., Cozzani, V., 2015. Hazard identification for innovative LNG regasification technologies. Reliab. Eng. Syst. Saf. 137, 18–28.
Pasman, H.J., 2015. Risk Analysis and Control for Industrial Processes-Gas, Oil and Chemicals: A System Perspective for Assessing and Avoiding Low-Probability, High-Consequence Events. Butterworth-Heinemann.
Rodriguez, M., Diaz, I., 2016. A systematic and integral hazards analysis technique applied to the process industry. J. Loss Prev. Process. Ind. 43, 721–729.
Rausand, M., 2013. Risk Assessment: Theory, Methods, and Applications. John Wiley & Sons.
Rokseth, B., Utne, I.B., Vinnem, J.E., 2017. A systems approach to risk analysis of maritime operations. Proc. Inst. Mech. Eng. O J. Risk Reliab. 231 (1), 53–68.
Saheed, Z.S., Egwaikhide, C., 2012. Impact of social crises on economic development: theoretical evidence from Nigeria. Am. Int. J. Contemp. Res. 2, 176–184.
Stamatis, D.H., 2003. Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press.
Thomas, J., 2013. Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis. Massachusetts Institute of Technology.
Wutc, P., 2016. Failure Investigation Report – Liquefied Natural Gas (LNG) Peak Shaving Plant. Williams Partners Operating, LLC, Plymouth, Washington.
Young, W., Leveson, N.G., 2014. An integrated approach to safety and security based on systems theory. Commun. ACM 57, 31–35.

Paper II

Sharmin Sultana, Vinnem Jan Erik, Jan Dahlsveen, Stein Haugen. Inherent safety assessment: current state of the art and why it is still not effectively adopted by industry. The 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference. 2020. Italy: Research Publishing, Singapore.

Inherent safety assessment: current state of the art and why is still not effectively adopted by industry

Sharmin Sultana
Department of Marine Technology, NTNU, Norway, Email: sharmin.sultana@ntnu.no

Jan Erik Vinnem
Department of Marine Technology, NTNU, Norway, Email: jan.erik.vinnem@ntnu.no

Jan Dahlsveen
Safetec Nordic AS, Sluppenvegen 6, 7037 Trondheim, Norway, Email: jan.dahlsveen@safetec.no

Stein Haugen
Department of Marine Technology, NTNU, Norway, Email: *stein.haugen@ntnu.no*

Abstract
Inherent safety is a proactive approach to risk reduction. The industry should adopt it in the early stages of design as it is the most prominent approach to risk reduction, as described by experts. Researchers have worked on this concept for a long time. There has been a lot of work on inherent safety evaluation techniques, including quantitative index-based and consequence-based evaluation or qualitative methods. The index-based inherent safety evaluation methods may not help users to understand the hazards fully evolved by each process route because the exact cause of the hazards may remain unknown to the users. Many times, it is not clear which of several process alternatives is inherently safer. Often the evaluation approach may limit the users only to choose one option among several, rather than improving further on the selected one. Improved methods are needed, along with inherent safety ranking among several alternatives and for improvement of the selected one at the same time. The scope of inherent safety design should not include accident prevention or reduction; of course, it should be a part of overall risk management. The paper aims to frame the current state of the art of inherent safety evaluation work, the limitations, and conflicts in their practical application in industry.

Keywords: Inherent, Safety, Inherently, Safer, Industry, Chemical, Risk.

1. Introduction

Inherent safety (IS) is a proactive approach to process safety by which hazards are eliminated or lessened to reduce risk without any engineered or procedural intervention. Researchers have done a lot of work on inherent safety and on methods to measure inherently safer design. Still, after many years, no evaluation method is adopted widely in the industry. The paper aims to analyse possible reasons for slow adoption and present proposals in short for improvement in the future. The present work is based on existing literature, including journal papers, existing codes and standards.

Gupta and Edwards (2002) performed a questionnaire-based review work to find the status of Inherently Safer Design (ISD) and its application. Available indices at that time were Dow's fire and explosion index; Dow's chemical exposure index; Mond's fire, explosion, and toxicity index; mortality index; hazard identification and ranking index (HIRA); safety weighted hazard index; inherent safety index. After their work, several case studies concerning index development or economic benefits have been performed.

Many responders of the survey, as carried out by Gupta and Edwards (2002), said that they were familiar with the concept of IS indices but did not use them. The reasons were that the IS indices were too complicated. It requires much data that need to be processed manually and is challenging to use in early development stages. The same reasons still exist at present.

Researchers have defined the terms inherent safety and inherently safer design in various ways. According to Kletz, inherent safety is to remove the hazards from the source rather than to control them. It is not possible to eliminate all potential hazards (Lees 2012). According to CCPS, a chemical manufacturing process is inherently safer if it reduces or eliminates the hazards associated with materials and operation used in the process permanently and inseparably. Rogers and Hallam (1991) give an alternative definition of inherent safety. They say that an inherently safe process is one which by its design, does not produce a hazard if a fault occurs. They discuss making a process inherently safer outside normal operation. IS approach of prevention tries to avoid or eliminate the hazards or reduce their extent,

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

severity, or likelihood of occurrence by attention to fundamental design and layout (Khan, Sadiq and Amyotte 2003).

Many researchers have worked on evaluation techniques for inherent safety assessment. The industry is yet not ready to use any of them. An efficient qualitative method may help the user to choose the inherently safer option quickly. The industry is reluctant to use cost and time to do any additional assessment. Quantitative methods that involve too much calculations, also need an expert resource to perform them. A qualitative method that accounts for all the elements of inherent safety in an easy way may help. Section 2 of the paper discusses earlier inherent safety assessment works. Chapter 3 discusses the shortcomings of various methods and concludes on future work.

2. Previous works

T. Kletz (1978) first introduced the concept of the inherent safety in his lecture 'what you do not have, can't leak.' He emphasized removing the source of hazard to establish a safe chemical plant rather than to control it. Kletz (1985) had adopted four principles as an inherent safety strategy. The principles were intensification, substitution, attenuation, and simplification. Later Kletz has presented several publications (Kletz 1991; 1996; 1998; 2002; Kletz and Amyotte 2010) describing this concept and its application procedure.

2.1 Consequence based quantification of inherent safety.

Consequence-based methods quantify damage potential without quantifying the probability of accidents occurring. Deterministic equations determine the consequence, and design solutions are compared based on that.

2.1.1 Dow F&EI hazard index

This index, proposed by Dow chemicals and AICHE (1987), was used first as a measure of inherent safety implementation. It quantifies damage due to fire and explosion and identifies the most contributing equipment for the accident during the operation. The Dow index is the product of material factor and process unit hazard factor. The material factor is a measure of potential energy released from material by considering the flammability and reactivity of material. The process unit hazard factor is the product of the two penalty factors. Penalty factors include consideration for both general process hazards and special process hazards. Gupta (1997), Suardin, Sam Mannan and El-Halwagi (2007), Gupta, Khemani et al. (2003) and Nezamodini, Rezvani and Kian (2017) has used Dow index for ISD evaluation. When using the Dow index to check the ISD option, analysts determine the Dow index for both based design and actual design. An alternate solution is proposed based on that.

2.1.2 Mond index

The initial hazard assessment described in the Mond index (Lewis 1979) is similar to the Dow index, but it considers additional hazards. Potential hazards in this method are due to fire, explosion, and toxicity. Material factors, general process hazards, and special process hazards are almost the same. It uses a quantity factor, based on an inventory of material, layout hazard factor, and toxicity hazards. This method calculates the toxicity index by using a health factor, the number of chemicals in use, and the toxicological properties of the substances. Furthermore, this method introduces a hazard offsetting factor, which includes preventive measures to reduce the frequency of incidents, and for mitigation of consequences. Further work with the Mond index is the work of Tyler (1985) and Tyler et al. (1994).

2.1.3 SHE indexes

This method (Koller, Fischer and Hungerbühler 2000) defines Fate indices representing corresponding SHE effects. Identified dangerous properties are mobility, fire or explosion, reaction or decomposition, and acute toxicity, air mediated effects, solid waste, degradation, etc. The value of these dangerous properties depends on related SHE effects e.g. fuel, ignition source, oxygen source, thermal stability. The resulting potential danger represents the magnitude of the SHE aspect, indicating the releasable energy content of a system. The total SHE effects are the summation of the potential threat of all substances. The last step of the assessment considers technologies provided to reduce SHE problems. Each technology factor reduces the potential danger depending on the effectiveness of the technology.

2.1.4 Safety weighted hazard index (SWeHI)

SWeHI (Khan, Husain and Abbasi 2001) represents the radius of the area under hazard due to the given unit/plant, considering the chemicals, operating conditions, and environmental settings involved at that instant. SWeHI identifies two factors; the first one is a quantitative measure of the damage that may be caused by a unit/plant, measured in terms of area under a 50% probability of loss. The second factor presents the credits due to control measures and safety arrangements made to prevent undesirable situations. The action

of damage has two components. The first one is to address damage due to fire and explosion. The second one considers damage due to toxic release and dispersion. Various units of industry, e.g., storage unit, heat transfer, mass transfer unit, pump, compressor, furnace, boilers, are considered by classifying into various categories based on their damage potential.

2.1.5 Integrated inherent safety index (I2SI)

I2SI (Khan and Amyotte 2004) considers the life cycle of the process with economic evaluation and hazard potential identification for each option. It is composed of sub-indices for hazard potential, inherent safety potential, and adds on control requirements. Hazard potential index (HI) calculation includes a damage index and a process and hazard control index. The damage index is a function of four parameters: fire and explosion, acute toxicity, chronic toxicity and environmental damage. Damage radii need to be calculated using the SWeHI approach to get damage radius. The process and hazard control index depend on the control arrangements required. The inherent safety potential index accounts for the applicability of inherent safety principles to the process and any requirement to install an add-on process and hazard control measures after the implementation of the inherent safety measures. I2SI is the ratio of ISPI and HI. Higher the value of I2SI, more pronounce the inherent safety impact.

2.1.6 Toxic release consequence analysis (TORCAT)

TORCAT (Shariff and Zaini 2010), proposes a consequence analysis-based evaluation of ISD based on the worst-case scenario of toxic release. This method uses iCON, a process simulation software developed by Petronas, for the initial design of the process plant. Data for pressure, temperature, composition, heat capacities are extracted from iCON and inputted to MS-Excel for further consequence analysis. Process designers provide other data such as duration of release, hole diameter, and distance from the point of discharge based on worst-case scenarios. A toxic release consequence model, recommended by the Center for Chemical Process Safety (CCPS), calculates the dispersion of toxic release. A toxic gas effect model, developed by DNV, calculates the consequence analysis of toxic gas. The toxic effect model provides results of probit value and percent of fatalities.

2.2 ISD PARAMETERS BASED METHOD

This type of method starts by defining Kletz's principle: which is minimization, modification, substitution, simplification. Analysts search parameters to achieve these principles and set index-values for various ranges of all parameters. The overall index is normally a summation of all sub-indexes. Design alternatives are compared based on the determined index value. These methods depend highly on subjective judgment.

2.2.1 Prototype index of Inherent safety (PIIS)

Edwards and Lawrence (1993) are the first to present the index-based ranking of inherent safety evaluation among various process routes. Primarily, their method identifies 17 parameters affecting the inherent safety of a process from which they choose seven, which are most affecting. Possible ranges of each parameter are defined, and numerical values assigned to each subrange. The sum of the scores of parameters like pressure, temperature, and yield is the process score. The summation of the scores of flammability, toxicity, explosiveness, and inventory is the chemical score. The final score is the summation of these two scores, which is a measure of inherent safety. Heikkilä (1999) proposes a modified index of PIIS by altering scoring tables and adding a few more parameters, e.g., type of equipment, the safety of process structure, chemical interaction. She mentions strategies like intensification, substitution, attenuation, limitation of effects, simplification, making incorrect assembly impossible, tolerance, and ease of control as inherent safety principles, some of which are the characteristics of a friendly plant described by Kletz (Kletz 1989, 1990).

2.2.2 iSafe

This method (Palaniappan, Srinivasan and Tan 2002b; Palaniappan, Srinivasan and Tan 2002a) proposes three new supplementary indices known as the worst chemical index, worst reaction index, and total chemical index to overcome the shortcoming of earlier indices. They developed an expert system for the application of inherent safety in chemical process design. The authors compared three different routes for producing phenols using the method to identify inherent safety issues and to generate inherent safety alternatives.

2.2.3 Qualitative assessment for inherently safer design (QAISD)

QAISD method (Risza and Shariff 2010), consists of two stages- identification of inherent hazard

and generation of ISD options. Detailed analysis of hazards is carried out for each process unit to search for possible ISD solutions. This method uses two sub tools for the assessment, RIP (Register, Investigate and Prioritise) and IDH (Inherent, Design, Heuristic). The first task, Register, develops a heuristic process model for a processing unit considering design factor, process attribute, and hazard indicator. For the second task, Investigate, a hazard review method, Predictive Failure Analysis (PFA), is modified to suit QAISD methodology. The third task, Prioritise, is to identify the dominant hazards because not all predicted hazards are necessarily hazardous and could lead to the cause of consequences. Stage II, IDH, is the generation of ISD options. IDH stage makes as many as possible ISD options based on the ISD concept to eliminate or reduce the inherent hazards.

2.3 RISK-BASED INHERENT SAFETY INDEX

In this type of method, both consequence and probability, hence the risk is quantified. They use the Kletz principle to determine overall risk reduction. Design solutions are compared based on the risk scores.

2.3.1 Process route index (PRI)

This method (Leong and Shariff 2009) is proposed for IS quantification to treat chemicals in a process system as individual components, not as a mixture, which was the case for PIIS, ISI and iSafe. The level of explosiveness is used for IS quantification for process route selection to illustrate the importance of the individual contribution of components in a mixture. A crucial parameter is combustibility which is the difference between the lower flammability limit (LFL) and upper flammability limit (UFL). It determines an overall index (PRI) for each process route, which is a function of mass heating value, fluid density, pressure and flammability limit of the mixture.

2.3.2 Inherent risk assessment (IRA)

IRA (Shariff and Leong 2009) estimates the inherent risk of the selected process route due to its design and chemical used to remove the limitation of Quantitative risk assessment (QRA), which is only applicable at later stages of process design. Here, the risk assessment tool is integrated with the process design simulator (HYSYS) to provide necessary process data early at the process design stage. The risk assessment tool consists of two components to calculate probability and consequence relating to possible risk due to significant accidents. Analysts compare risk factors for various design solutions and propose modifications accordingly. This method estimates risk as a function of probability or frequency and consequences, and a two-region FN curve to represent an inherent risk. Two regions cover 'tolerable if ALARP' and 'tolerable.' Like QRA, it does not require safety control measures such as procedure and instrumented protective functions.

2.3.3 Risk-based inherent safety index (RISI)

This (Rathnayaka, Khan and Amyotte 2014) is a risk-based design decision-making tool considering inherent safety. It incorporates both the consequence and probability of accident occurrence reduction through the application of ISD throughout the process design life cycle. Analytical and subjection equations assess damage potential of major process accidents: fire, explosion, toxic release. RISI comprises of two distinct risk elements: base design risk (RiskBD) and inherent safety risk (ISRisk). The RISI is the ratio of the inherent safety risk of the selected alternative to the risk of the base design. After completion of the base design, carried by the design team, hazard identification identifies all potential inherent hazards associated with the base design and subsequently develop alternative models. Fire, explosion and toxic releases are studied considering most contributors for the occurrence of an accident in the process industry. Analysts analyse accident scenarios to construct an accident sequence.

2.3.4 Toxic release inherent risk assessment (TRIRA)

The TRIRA method (Shariff 2013) determines the toxicity risk levels using a 2-region risk matrix concept at the preliminary process design stage. This method determines the inherent risk due to the inherent properties of the chemicals involved and the process conditions of the design. TRIRA only focuses on the toxicity parameter and uses a process design simulator with an inherent risk assessment spreadsheet for data analysis.

2.4 EVALUATION OF INHERENT SAFETY BY GRAPHICAL ANALYSIS

The starting point of this type of method is the same as the 'ISD parameter-based' method. The difference is that the total index value is not determined. Analysts make the comparison by plotting different parameter relevant to the inherent safety.

2.4.1 Graphical method

This method (Gupta and Edwards 2003) is the first qualitative method for the evaluation of various routes from inherent safety point of view for comparison. The range of parameters for each route is determined first which may affect safety, for example, temperature, pressure, toxicity, flammability, etc. This method plots the values for comparison without carrying out any mathematical operation. All the plotted numbers are dimensionless. Analysts need to plot Fire, explosion, toxicity (FET) values as the sum of the highest importance for FET in that route. Another graphical method GRAND (Ahmad, Hashim et al. 2015) uses the logistic function for IS assessment. GRAND is useful to identify hazards posed by each route that contributed to chemical parameters and operating conditions.

2.4.2 Numerical descriptive Inherently safer design (NuDIST)

NuDIST method (Ahmad, Hashim and Hassim 2014) uses a logistic equation to eliminate subjective scaling of the index-based method. It consists of two parts: process safety and chemical safety. Chemical safety assessment considers four parameters: flammability, explosiveness, toxicity, and reactivity. Process safety parameters are temperature, pressure, the heat of reaction, and process inventory. After sorting all data into their range, the method builds a single number of frequencies for each interval. The cumulative curve for each parameter is developed by plotting data ranges against frequency calculated.

2.5 SYSTEM ENGINEERING-BASED APPROACH

This approach is quite a new approach where system engineering tools are applied to determine inherent safety applications.

2.5.1 RiskSOAP method

RiskSOAP (Chatzimichailidou and Dokas 2016) presents a STAMP-based indicator of measuring the inherent system design and development. The RiskSOAP methodology follows three already existing approaches: (1) the STAMP Based Process Analysis (STPA) (Leveson 2011); (2) the Early Warning Sign Analysis based on the STPA (EWaSAP) approach (Dokas, Feehan and Imran 2013) and (3) a binary dissimilarly measures method (Zhang and Srihari 2003). Risk SOAP is a method to measure the system's capability to sense and comprehend its vulnerabilities. The method goes through three main stages: define the ideal design version of the system, identify the real one, employ a comparative strategy aiming to depict the distance between two design versions and interpret the distance value. The capability of each system part to provide its agent the Situation Awareness (SA) about the presence of system threats and vulnerabilities that may lead to accidents is called risk situation awareness provision (RiskSOAP).

3. Discussion

In the previous section, we have reviewed various IS assessment techniques. This section aims to describe some limitations of existing approaches and present suggestions on a possible future tool that can be used. Some consequence-based methods e.g., Dow F& EI and Mond index, are not usable in the early stage of process design (Rahman, Heikkilä and Hurme 2005). Dow index is easier to use compared to Mond index and more systematic (Khan, Sadiq and Amyotte 2003). The results are difficult to interpret. Does better value mean less damage potential from fire or explosion? All aspects of inherent safety e.g., layout, complex interaction, cannot be considered by this approach. Dow and Mond index requires greater rigor, accuracy and precision in quantifying the impact of safety measures on the values of hazard indices (Khan, Husain, and Abbasi 2001).

SWeHI is more systematic and reliable for hazard identification, takes account of a large number of parameters for hazard quantification. It considers all the control measures adopted by the industry to mitigate a hazard. On a comparison between SWeHI and Dow index by (Khan, Sadiq and Amyotte 2003), authors found that none of them can capture all the inherent safety guidewords. They also found that the Dow index, SWeHI, ISI showed no change in values when the reactor type was changed. I2SI is not flexible enough when applied to different stages of the process design life cycle. TORCAT can support reduction of the severity of consequence by using inherent safety principles during the preliminary design stage. Modification of design is easy since TORCAT provides direct link between process design simulation and consequence model

ISD parameter-based index involves expert judgment of relative importance of various types of hazards. The result may become different, due to different experience and competence of the experts. Another limitation of existing approaches of this type (e.g., ISI, SHE) is that they do not consider the interaction between different factors. They are not flexible enough to incorporate additional available data. Parameters established for a specific type of industry may not be relevant for another industry. Different types of hazards

may become dominant for different applications. How to include this type of additional hazard to an existing approach (e.g., PIIS, ISI) is a question. SHE index does not find hazards related to equipment, their configuration and the complexity of the process.

Another problem of this type of method is that they (e.g., PIIS, ISI) make a sudden jump in the score value at the sub-range boundaries. For example, according to PIIS, for a temperature range 100 to 199, the score is 2, while for a temperature range 200 to 299, the score is 3. This may also be the case for other parameters, like pressure, inventory, no of steps etc. A process getting a score of two is not guaranteed to be better than an alternative getting score 3. This type of indexing cannot consider all aspects of safety. A route with two steps may not be twice as bad as a single step, whereas while indexing a two-step process is given a lower score than a unique step process. A multi-step process can be better than a single-step, high-hazard process (Heikkilä 1999). Small inventories of chemicals do not assure that it is safer than a large inventory. The index-based approach does not help the user to fully understand the hazards evolved in each process routes as it does not discuss the exact cause of hazards.

Another problem with this type of method is the dimensionality problem (Gupta and Edwards 2003). Adding parameters of different dimensions like temperature (◦C), pressure (atm), inventory (t), toxicity (ppm) and comparing the summed value may become unacceptable scientifically from the chemical engineering point of view and making terms dimensionless means that temperature and pressure in a range should pose the same level of hazard. This implies a predefined equality of hazard rating which is considerable and cost demanding task also.

In a comparison of four methods, PIIS; iSafe, ISI, QAISD, (Rahman, Heikkila and Hurme 2005), it was found that they all have some limitations. PIIS does not consider heat of reaction, reactivity, equipment, process type hazards and has too steep temperature index. A good point of PIIS is that it is very straightforward and fast to use, and all the input data is obtainable from material safety data sheets and process literature. iSafe lack inventory, equipment and process sub-indices. ISI has the most extensive set of sub-indices; more factors are covered. The downside is that the evaluation of sub-indices is laborious. PIIS, ISI and iSafe treat chemicals as individual components, not as a mixture. They cannot reflect the contribution of different elements in the mix.

Risk-based approaches are useful in the sense that the overall goal is to reduce risk. Risk can be compared for various designs and can be modified accordingly. The process route index is useful to rank between different chemical process routes. However, it only considers explosion potential so that another remaining hazard potential will remain outside the scope of analysis.

Results from Inherent risk assessment (IRA) are suitable to be used as a quantitative method to screen processes and provide judgments for design improvements at the early design stage. If integrated with process design simulation (e.g., HYSYS), it evaluates ISD options in a short time, I.e., inherent risk before and after pressure modification of a unit operation can be promptly assessed. However, industry personnel may not be interested in using such a tool in addition to QRA, as there is no regulatory requirement and industry has used QRA for a long time. Additional cost, time and need for expert resources may discourage them from using such a tool. The same factors apply to the Risk-based inherent safety index (RISI). RISI is applicable at different stages of the process design life cycle. The problem with the Toxic Release Inherent Risk Assessment (TRIRA) is that it only considers toxic risk levels. The integrated risk estimation tool (Shariff et al. 2006) does not give enough information about achieving an inherently safer design of the process based on parameter modification.

RiskSOAP is useful as a selection criterion between alternative designs of the same or different systems or as a decision-making tool between the alternative method. In case of any change in the controls of the examined system or system part, an analysis should run the methods STPA and EWaSAP again. Setting a threshold value for risk situation awareness (SA) provision capability requires subjective interpretation, so it may differ from system to system and from designer to designer, affecting the degree of design modifications. Another limitation is the overabundance of dissimilarity measures that hinder the decision to select a suitable measure toward achieving goals. RiskSOAP uses a binary-based indicator, neglecting that variables may have an exact value between 0 and 1. No weight is assigned to the critical system elements since they are treated as equivalent to the enhancement or degradation of RiskSOAP capability (Chatzimichailidou and Dokas 2016).

One reason why the industry has been slow to implement the use of any of these methods is the lack of expertise for users to use them. A second reason is the complexity to implement them in practical cases. Industry personnel is unable to understand the necessity of using such a tool.Another reason is the lack of information to set the parameter value. Index values (e.g., chemical interaction, correction) are not readily

available (Rahman, Heikkilä and Hurme 2005). Evaluation of the process concept index is very experience-based. All methods suffer from a lack of sub-index interaction (Rahman, Heikkilä, and Hurme 2005).

Choosing the best option between two conflicting actions is a critical task. Most of the methods are applicable later in the design sequence, which requires detailed data and time. It is difficult to use them in the early design stage when there is enough leverage to make changes to lead to the design of the safer plant.

4. Conclusion

This paper has reviewed previous literature on inherent safety assessment techniques and tried to find the limitation of these to use them in industry. Undoubtedly, a lot of work has been done. However, still, the industry is reluctant to use them due to time and cost constraints. A qualitative method may encourage the user who needs less time, cost and resource. Future work is required to establish an efficient qualitative method that can account for all the elements of inherent safety. Users should be able to use inherent safety principles at the initial design stage and to rank them easily without doing any additional calculation. The tool should have characteristics from which people can interpret results easily and can find interrelationships between multiple entities. Possible future work may help the industry in this regard.

Acknowledgment

The authors like to thank the Norwegian Research Council and DynSoL AS for their financial support for this work through project number 283861.

References

Ahmad, Syaza I, Haslenda Hashim, and Mimi H Hassim. (2014). Numerical Descriptive Inherent Safety Technique (NuDIST) for inherent safety assessment in the petrochemical industry. *Process Safety and Environmental Protection* 92 (5): 379-389.

Chatzimichailidou, Maria Mikela, and Ioannis M. Dokas. (2016). RiskSOAP: Introducing and applying a methodology of risk self-awareness in road tunnel safety. Accident Analysis and Prevention 90: 118-127.

Chatzimichailidou, Maria Mikela, and Ioannis M. Dokas. (2016). Introducing RiskSOAP to communicate the distributed situation awareness of a system about safety issues: an application to a robotic system. Ergonomics 59 (3): 409-422.

Dow Chemical, and American Institute of Chemical Engineers. (1987). Fire & explosion index: hazard classification guide. American Institute of chemical engineers.

Dokas, Ioannis M, John Feehan, and Syed Imran. (2013). EWaSAP: An early warning sign identification approach based on systemic hazard analysis. Safety science 58: 11-26.

Edwards, David W, and Duncan Lawrence. (1993). Assessing the inherent safety of chemical process routes: is there a relation between plant costs and inherent safety? Process Safety and Environmental Protection 71 (B4): 252-258.

Gupta, Jai P, G Khemani, and M Sam Mannan. (2003). Calculation of Fire and Explosion Index (F&EI) value for the Dow Guide taking credit for the loss control measures. Journal of Loss Prevention in the Process Industries, 16: 235-41.

Gupta, JP. (1997). Application of DOW's fire and explosion index hazard classification guide to process plants in the developing countries. Journal of Loss Prevention in the Process Industries, 10: 7-15.

Gupta, JP, and DW Edwards. (2002). Inherently safer design—present and future. Process Safety and Environmental Protection, 80: 115-25.

Gupta, J. P., and David W. Edwards. (2003). A simple graphical method for measuring inherent safety. Journal of Hazardous Materials 104 (1-3): 15-30.

Heikkilä, Anna-Mari. (1999). Inherent safety in process plant design: an index-based approach. VTT Technical Research Centre of Finland.

Hurme, M., and M. Rahman. (2005). Implementing inherent safety throughout process lifecycle. Journal of Loss Prevention in the Process Industries 18 (4-6): 238-244.

Izyanni Ahmad, Syaza, Haslenda Hashim, and Mimi Haryani Hassim. (2015). Graphical Technique for Root-Cause Analysis in Inherent Safety Assessment. Advanced Materials Research, 1113: 723-732.

Khan, F. I., T. Husain, and S. A. Abbasi. (2001). Safety Weighted Hazard Index (SWeHI): A New, User-friendly Tool for Swift yet Comprehensive Hazard Identification and Safety Evaluation in Chemical Process Industrie. Process Safety and Environmental Protection 79 (2): 65-80.

Khan, Faisal I., Rehan Sadiq, and Paul R. Amyotte. (2003). Evaluation of available indices for inherently safer design options. Process Safety Progress 22 (2): 83-97.

Khan, Faisal I., and Paul R. Amyotte. (2004). Integrated inherent safety index (I2SI): A tool for inherent safety evaluation. Process Safety Progress 23 (2): 136-148.

Khan, Faisal I., Rehan Sadiq, and Paul R. Amyotte. (2003). Evaluation of available indices for

inherently safer design options. Process Safety Progress 22 (2): 83-97.

Kletz, Trevor A. (1978). What you don't have, can't leak. Chemistry and Industry, 6: 287-92.

Kletz, T., (1991). Inherently Safer Plants - Recent Progress. Hazards Xi: New Directions in Process Safety: 225-233.

Kletz, T., (1996). Inherently safer design: The growth of an idea. Process Safety Progress 15 (1): 5-8.

Kletz, T., (2002). Past, present, and future - Inherent safer design. Nuclear Engineering International 47 (570): 46-47.

Kletz, T. A., (1985). Make Plants Inherently Safe. Hydrocarbon Processing 64 (9): 172-&.

Kletz, T. A., (1989). Friendly Plants. Chemical Engineering Progress 85 (7): 18-26.

Kletz, T., (1990). The Need for Friendly Plants. Journal of Occupational Accidents 13 (1-2): 3-13.

Kletz, Trevor, A. (1998). Process plants: a handbook for inherently safer design. Philadelphia, PA: Taylor & Francis.

Kletz, Trevor A., and Paul Amyotte. (2010). Process plants: a handbook for inherently safer design. 2nd ed. text. Boca Raton, FL: CRC Press/Taylor & Francis.

Koller, Guntram, Ulrich Fischer, and Konrad Hungerbühler. (2000). Assessing safety, health, and environmental impact early during process development. Industrial & Engineering Chemistry Research 39 (4): 960-972.

Lees, Frank. (2012). Lees' Loss prevention in the process industries: Hazard identification, assessment, and control. Butterworth-Heinemann.

Leong, Chan T, and Azmi Mohd Shariff. (2009). Process route index (PRI) to assess level of explosiveness for inherent safety quantification. Journal of Loss Prevention in the Process Industries, 22: 216-21.

Leveson, Nancy. (2011). Engineering a safer world: systems thinking applied to safety. MIT press.

Lewis, DJ. (1979). The Mond Fire, Explosion and Toxicity Index-a Development of the Dow Index. Proceedings of the AIChE on loss prevention symposium, New York.

Nezamodini, Zeynab Sadat, Zahra Rezvani, and Kumars Kian. (2017). Dow's fire and explosion index: a case study in the processing unit of an oil extraction factory. Electronic physician 9 (2): 3878.

Palaniappan, Chidambaram, Rajagopalan Srinivasan, and Reginald Tan. (2002a). Expert system for the design of inherently safer processes. 1. Route selection stage. Industrial & engineering chemistry research 41 (26): 6698-6710.

Palaniappan, Chidambaram, Rajagopalan Srinivasan, and Reginald B Tan. (2002b). Expert system for the design of inherently safer processes. 2. Flowsheet development stage. Industrial & engineering chemistry research 41 (26): 6711-6722.

Rahman, Mostafizur, Anna-Mari Heikkilä, and Markku Hurme. (2005). Comparison of inherent safety indices in process concept evaluation. Journal of Loss Prevention in the Process Industries 18 (4-6): 327-334.

Rathnayaka, S., F. Khan, and P. Amyotte. (2014). Risk-based process plant design considering inherent safety. Safety Science 70: 438-464.

Rogers, R. L., and S. Hallam. (1991). A Chemical Approach to Inherent Safety. Process Safety and Environmental Protection 69 (B3): 149-152.

Rusli, Risza, and Azmi Shariff. (2010). Qualitative assessment for inherently safer design (QAISD) at the preliminary design stage. Journal of Loss Prevention in the Process Industries 23 (1): 157-165.

Shariff, Azmi Mohd, and Chan T Leong. (2009). Inherent risk assessment—a new concept to evaluate risk in the preliminary design stage. Process Safety and Environmental Protection 87 (6): 371-376.

Shariff, Azmi Mohd Zaini. (2013). Inherent risk assessment methodology in the preliminary design stage: a case study for toxic release. Journal of Loss Prevention in the Process Industries 26 (4): 605-613.

Shariff, Azmi Mohd, and Dzulkarnain Zaini. (2010). Toxic release consequence analysis tool (TORCAT) for inherently safer design plant. Journal of hazardous materials 182 (1): 394-402.

Shariff, Azmi, Risza Rusli, Chan T. Leong, V. R. Radhakrishnan, and Azizul Buang. (2006). Inherent safety tool for explosion consequences study. Journal of Loss Prevention in the Process Industries 19 (5): 409-418.

Suardin, Jaffee, M. Sam Mannan, and Mahmoud El-Halwagi. (2007). The integration of Dow's fire and explosion index (F&EI) into process design and optimization to achieve the inherently safer design. Journal of Loss Prevention in the Process Industries 20 (1): 79-90.

Tyler, BJ. (1985). Using the Mond Index to measure inherent hazards. Process Safety Progress, 4: 172-75.

Tyler, BJ, AR Thomas, P Doran, and TR Greig. (1994). A toxicity hazard index. Institution of chemical engineers symposium series.

Zhang, Bin, and Sargur N Srihari. (2003). Properties of binary vector dissimilarity measures. Proc. JCIS Int'l Conf. Computer Vision, Pattern Recognition, and Image Processing.

Paper III

Sultana, S., Haugen, S.., Achieving inherent safety from hazard and risk factors. In 31st European Safety and Reliability Conference ESREL 2021. Trondheim, Norway (Sultana and Haugen, 2021).

Achieving inherent safety from inherent hazard and risk factors

Sharmin Sultana

Department of Marine Technology, Norwegian University of Science & Technology, NTNU, Norway, email: sharmin.sultana@ntnu.no

Stein Haugen

Department of Marine Technology, Norwegian University of Science & Technology, NTNU, Norway, email: stein.haugen@ntnu.no

Inherent safety is considered the best approach to risk reduction. Academia and industry personnel have studied this topic for a long time. However, many misconceptions and lack of clarity still exist in the industry. Also, there have been many variations in defining the concepts and principles of inherent safety. The paper aims to analyse the concept in a novel way after reviewing past works on the inherent safety concept. The work focuses on the in-depth and systematic identification of hazards for better understanding. It seeks the factors contributing to creating the hazard to propose inherent safety measures. Identifying inherent hazard and risk factors makes it easier for the user to quickly find an inherently safer solution. This approach draws a clear distinction between three risk reduction measures, inherent, passive and active. Inherent safety measures try to reduce the hazard from origin or try to attenuate inherent hazard and risk factors, while passive and active measures only focus on reducing the consequences of accidents or hazardous events. They do not intend to reduce the inherent hazard and risk factor from the system. This paper presents a new definition of inherent safety with a new perspective and identifies the principles used to achieve inherent safety.

Keywords: inherent safety; inherently safer; hazard; risk management; chemical process and systems; oil and gas industry.

1. Introduction

Inherent safety (IS) is the best approach to risk reduction as the best way to deal with safety problems is to eliminate the problem from the source or avoid a critical situation before it arises. An inherently safer design avoids hazards instead of controlling them by reducing hazardous material and the number of hazardous operations in the plant (Heikkilä, 1999). It is a proactive way of addressing risk. It is also cost-effective since it eliminates the need for expensive layers of protection. If successfully applied, this approach contributes to less energy use, less maintenance, less waste and reduced pollution (Gupta and Edwards, 2002, Abedi and Shahriari, 2005).

Earlier disasters such as Flixborough, Seveso, and Bhopal have drawn attention to the need to apply inherent safety principles. The Bhopal disaster in 1984 occurred due to a leak of an intermediate methyl isocyanate, which could have been removed instead of storing it (Shrivastava, 1992). Proper application of IS could lead to identifying this solution during the plant's design phase. In the Richmond refinery accident of 2012, severe Sulphidation corrosion was the root cause of an accident due to using an inherently unsafe construction material for a pipe (Grim et al., 2015).

The Seveso accident in 1976 occurred during the production of TCP (2,4,5-trichlorophenol). The unexpected exothermic reaction caused an increase in temperature, slow decomposition of reaction mass, gas formation, and a rise in pressure (Sambeth, 1982). In 1984, there was an explosion at the Pemex LPG terminal in Mexico City. Destruction of the terminal occurred because there was a failure of overall risk management, including the plant's layout and emergency isolation features (Pietersen, 1988). Terminal's active safety measures firewater system was disabled in the initial blast, and water spray was inadequate. Traffic chaos obstructed the way of the emergency rescue service. This massive incident points to the necessity of inherent safety measures ahead of passive and active measures, as active systems can fail at any time.

Incorporating inherent safety into the chemical process at the design stage is challenging due to possessing limited process information. Identifying relevant hazards for different scenarios and processes is always critical (Eljack et al., 2019). One of the drawbacks of inherently safer design (ISD) is risk transfer, as reducing one hazard may introduce or increase another hazard. Therefore, it is crucial to understand the properties of chemicals and systems that make them hazardous (Ade et al., 2019).

Lack of awareness about ISD, lack of actual case studies on ISD implementation, difficulty in implementation in an existing plant, lack of formal regulation on ISD philosophy are barriers to broad adoption of ISD (Jafari et al., 2018). Most of the earlier methods focus on selecting alternative process route considering IS indexing. Sometimes, managers focus on ensuring the plant's overall safety, giving the same priority to inherent, passive and active measures, although the three should not carry the same importance during plant design (Kletz, 1985c). Kletz (1978a), a pioneer of inherent safety, proposed four main principles to achieve inherent safety. These are intensification, modification, substitution and simplification. He and later researchers have shown the inherently safer design process by using these principles. However, how these principles can affect the inherent hazard and risk factors demand more study.

The study focuses on the chemical and mechanical processing industry and applicable inherent safety measures at the design stage. The paper's primary objective is to propose a concept to achieve ISD based on identifying

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer
Published by Research Publishing, Singapore.
ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_489-cd

inherent hazard and risk factors. The method tries to find hazards from the source systematically. Then the findings can be used to find inherently safer solutions. It gives a theoretical explanation of various risk reduction measures. Section two of the paper discusses earlier work in the field of inherent safety. Section three describes the concepts of hazard and hazardous events (HEs) with examples. Section four presents the new definition of IS and discusses the differences between the three types of risk-reducing measures. Section five identifies various principles which can be applied to achieve IS of a system, and the results are discussed in section six. The conclusion in section seven presents a summary of the present work and guides toward possible future work.

2. LITERATURE REVIEW

Many studies have been done on the topic of inherent safety, including the evaluation of inherent safety assessment, both qualitatively and quantitatively. The most outstanding efforts for inherent safety have come from Kletz. He has worked on hazardous materials (1977), process hazard (1985a), onshore, offshore hazard (1993) and hazard analysis for various applications (1978b). Other notable works are the works of Hendershot (1997), Mansfield and Cassidy (1994), Englund (1995) and Khan and Amyotte (2003).

Various researchers have defined IS in different ways. According to Kletz, *inherent safety is to remove the hazard from the source rather than try to control them* (Kletz, 1985c). Kletz defined hazard as a substance, object or situation that can give rise to injury or damage (Kletz, 1999). According to Kletz, extensive inventories of toxic or flammable materials are inherently unsafe, while small inventories of non-toxic or non-flammable material are inherently safer. He adopted four basic principles as an inherent safety strategy; substitution, intensification, attenuation, and simplification (Kletz, 1985b). The first choice should be to remove the hazard 'as much as reasonably practicable' (Kletz, 2004). If we cannot remove the hazard, our next choice should be to keep it under control by adding passive protective equipment. Kletz (1988) proposed the idea of a 'friendly plant', including some other principles to the IS principles, e.g., avoiding knock-on effects, incorrect assembly impossible, status clear, error tolerance, more comfortable to control, software, vice versa. He gives more application examples for the chemical and nuclear industry (Kletz, 1998).

According to Hendershot (1997), a chemical manufacturing process could be described as inherently safer if it reduces or eliminates one or more hazards associated with the materials and operations used in the process than some alternative processes. This reduction or elimination should be inseparable and implementable as a permanent system characteristic (Hendershot, 1997). He defined hazards as basic properties of material or conditions of usage. The inherent safety approach reduces or eliminates hazards by reducing hazardous material or energy or eliminating the hazardous agent.

Khan et al. (2003) state that the IS approach of loss prevention tries to avoid or eliminate the hazards or reduce their extent, severity or likelihood of occurrence by attention to fundamental design and layout. Passive measures reduce or eliminate hazards by process and equipment design that reduce either incident frequency or consequences without any device's active functioning (Khan and Amyotte, 2005).

Inherent safety approach seeks to remove the hazard at the source instead of accepting the hazard and looking to mitigate the effects. To implement inherent safety, Tugnoli et al. (2008) consider domino hazard potential. Domino hazard reduction through IS will make addon measure less critical and more effective (Cozzani et al., 2007). Palaniappan et al. (2004) state that the term 'inherently safer' implies that the process is safe by its nature and not externally constrained to be safe using add-on systems and devices. According to Abedi and Shahriari (2005), inherent safety (primary prevention) develops technologies that prevent the possibility of a chemical accident. Layers of protection (secondary prevention) reduce the probability of a chemical accident, and mitigation and emergency responses reduce the seriousness of injuries, property and environmental damage. Rusli et al. (2013) say that ISD can alter hazard from one dimension to another dimension. ISD can form new hazards and can change the magnitude of the existing hazards. He proposes a tool to quantify the inherent hazard while selecting a design alternative. Ahmad et al. (2019) describe inherent safety as a safety program that prevents hazards from occurring instead of eliminating hazards upon being detected.

According to Edwards and Lawrence (1993), inherent safety is intrinsic to a plant. There should not be any accident in an inherently safe plant; even if they do, they are self-correcting or escalating harmlessly. The index for measuring inherent safety that they proposed incorporates judgement of relative importance of various hazards. According to Heikkila (1996), an inherently safer design avoids hazards instead of controlling them. Reducing the amount of hazardous material and the number of hazardous operations in the plant can avoid the hazard. Instead of assuming that we can keep large quantities of hazardous materials under control, we must remove them (Heikkila 1996).

Both Edwards and Lawrence (1993) and Heikkila (1996) chose IS parameters that significantly affect the degree of hazard and advise about IS principles to be followed based on the effect. They follow the strategy that the effect of parameters on the degree of hazard should be kept small. For example, the amount of toxic inventory has a significant effect on the degree of hazard, so the amount of toxic inventory should be kept small by following the IS principle 'intensification or minimisation'. The proposed IS index is based on these IS parameters. Some critical parameters are flammability, explosiveness, corrosiveness, toxicity, reaction rate, inventory, temperature, pressure, etc.

Other indexing methods considered material hazard, reaction hazard, individual equipment hazard, and other process-related hazards like Dow's index. Dow's fire and explosion index into process design and optimisation is integrated in the work of Suardin et al. (2007). They chose a reactor and distillation column as the case study and

developed Fire and Explosion Index (F&EI) expression due to pressure and material in process units. Gupta (1997) applied Dow's fire and explosion index in process plant design in developing countries. Mond index considers hazard, which is the same as described by the Dow index. Additionally, it considers layout hazards and toxicity hazards. Tyler (1985) used the Mond index to measure inherent hazards.

Mizuta and Nakagawa (2013) analysed hazards in a chemical plant to identify inherent safety measures for decreasing consequences considering a worst-case scenario. They plotted calculation results on a graph with fatalities and lethality distance on the axes. In this way, the hazard potentials of chemical plants are ranked. The method can analyse equipment's hazard potential. Bernechea and Viger (2013) presented a method for optimizing storage plants' design and minimizing the risk by calculating an ideal number of tanks. They applied the principles of mathematical optimization to quantitative risk analysis.

Several authors (Hame et al., 1980, Pohanish, 2005, Bernechea and Viger, 2013, Chan et al., 2014, Zaini et al., 2016, Pasha et al., 2017, Medina-Herrera et al., 2014, Qi et al., 2019, Chiappetta et al., 2006, Ohashi et al., 2012, Petrovic, 2014, Eini et al., 2018, Fei et al., 2018) have discussed inherently safer options and essential factors in designing various equipment, selecting materials of construction, and operating the plant with reduced risks. Qi et al. (2019) investigates ISD through process intensification and shows how intensification improves safety performance due to risk transfer. Summers (2018) shows how IS principles can improve the sustainability of an automated system.

The centre for chemical process safety (CCPS) has provided checklists describing common failure modes for equipment used in process industries. CCPS defines a hazard as an inherent physical or chemical characteristics that have the potential to cause harm to people, property or the environment (2009). According to CCPS, *a chemical manufacturing process is inherently safer if it reduces or eliminates the hazards associated with materials and operation used in the process permanently and inseparably* (2009). CCPS offers examples and suggestions for inherent, passive, active, and procedural approaches for overall risk reduction and describes IS review methods, tools, and strategies for the process's lifecycle.

British Petroleum (BP) has adopted CCPS's definition of inherent safety. BP defined hazard as, *'Condition or practice with the potential to cause harm to people, the environment, property, or company's reputation'* (BP, 2008). The goal they defined as fewer hazards, fewer causes, less severity, fewer consequences. They defined three safety measures through the project life cycle: inherent, engineered, and procedural safety measures for new technology development, facility modifications, changes in existing operations, etc. Equinor and ExxonMobil also emphasized that capturing, understanding, and handling the inherent risk for operational safety management and IS process design should be applied whenever reasonably practicable (Statoil, 2010) (Bahri et al., 2009).

Inherent safety has been introduced as a desirable principle by several national authorities, including the US Nuclear Regulatory Commission and the UK Health and Safety Executive (Mansfield et al., 1996). International Electrochemical Commission (IEC) encourage ISD by saying that safety is best achieved by IS process design and may be combined with a protective system to address any residual risk (IEC, 2020). The US Chemical Safety Board have published many accident investigations describing how the concept of inherent safety could be applied to avoid accidents. UK offshore regulation includes the demonstration of inherent safety such as the substitution of hazardous materials for less hazardous ones, avoiding undue complexity, allowance for human factors, minimizing risk, selection of construction materials, design of vessels and pipeline to minimize the effects of sources of deterioration (HSE, Hamdan, 2006). NORSOK Z013 states that the choice of compensating measures should give the highest priority to inherent safety actions (NORSOK, 2010).

3. Concepts of Hazard and Accidents

3.1. Hazard

Hazard is the *existence of factors* that has the potential to cause harm to people or the environment or asset. Hazard factors are the properties or conditions or causes that may cause harm. Something is hazardous if it constitutes a hazard by its intrinsic or chemical properties such as flammability, explosiveness or toxicity. Hazards can be related to machinery, equipment, system, reaction, procedure, or material. Petrol is hazardous, as it is flammable. Material may not be hazardous in the general case but may become so due to a state or condition change. Steam is hazardous as it contains high thermal energy while water is not.

Inherent hazard factors can be of two types: triggering inherent hazard factors and impacting inherent hazard factors. Triggering inherent hazard factors are those factors that can directly contribute to a hazardous event. The presence of motion creates kinetic energy that can cause a hazardous event. Motion is, therefore, a triggering inherent hazard factor. Impacting inherent hazard factors does not contribute to creating a hazardous event directly but indirectly affects the severity or probability of a hazardous event. The object's geometry affects the amount of kinetic energy and affects the related hazardous event's severity. There can be many inherent hazard factors in the industry. Examples are harmful intensive physical properties, harmful extensive physical properties, harmful chemical properties, consumption of material and energy, harmful emission, incompatibility, incomprehensibility, congestion, noise.

3.2. Inherent risk factors

An inherent risk factor is the quantitative expression of inherent hazard factors. Triggering and impacting inherent risk factors are the quantitative expression of triggering and impacting inherent hazard factor subsequently. So, modification of inherent risk factors increases the likelihood of occurrence or severity of a

hazardous event. Triggering inherent risk factors contribute to creating a hazardous event directly. Impacting inherent risk factors do not contribute to creating a hazardous event directly but may affect triggering inherent hazard factors or risk level in the system, so the probability or severity of hazardous event may change.

The conceptualization of inherent risk factors assumes that the risk level (in terms of a quantitative measure) is controllable by changing, managing or controlling the inherent risk factors. Potential triggering inherent risk factors are vessel type, vessel quality, geographical quality, weather quality, etc., for fire and explosion in marine vehicles (Stornes, 2015). For ship collision, important impacting inherent risk factors are competence, lack of awareness, inadequate teamwork, violation of checklist and procedure. Figure 1 shows the relationship between inherent hazard factors and risk factors.

FIGURE 2 shows THE inherent hazard and risk factors for a hazardous event, a person hit by a car. For a car accident, inherent hazard factors are the motion of the car and exposure of human. Inherent risk factors are the duration of exposure, speed of the car. If the speed of the car is high, the severity of the event will increase. If exposure is high, the probability will increase. With increasing severity of inherent risk factors, e.g., car motion increases or more exposure of people, severity and probability of a hazardous event will increase. Impacting inherent risk factors are those which may affect the event statistically. It has been seen that the probability of a car crash is high for young people and on busy roads. So, the age of the driver type of road is impacting inherent risk factors.

3.3. Hazardous Event

A hazardous event is the realisation of the combined effect of the inherent hazard and risk factors present in a system. There can be various inherent risk factors present in a system. A hazardous event occurs when inherent risk factors from various dimension coexist at the same time with specific values. For a leak, related inherent risk factors can be high pressure/high temperature/high flowrate, weak pipe joints. A leak occurs if the pressure exceeds the tolerance of the pipe joint. If contributing inherent hazard factors present in the system increases, the event's probability or magnitude will increase. With the increment of the severity of inherent risk factors, the magnitude or probability of events also increases. A hazardous event is a multidimensional array of all the inherent risk factors present in the system. A hazardous event will occur if the product of the inherent risk factors exceeds the threshold. Risk, which means probability and consequence of a hazardous event, is the function of the required inherent risk factors.

$$R(HE) = f(TIRF_1.TIRF_2 \dots IIRF_1.IIRF_2 \dots) \quad (1)$$

Here, $R(HE)$ is the risk of a hazardous event
$TIRF_1.TIRF_2$ ...are triggering inherent risk factors
$IIRF_1.IIRF_2 \dots$ are impacting inherent risk factors

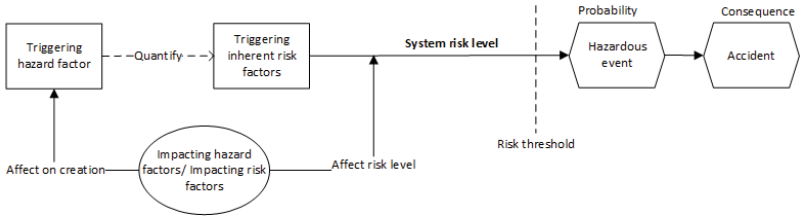


Figure 1: Relationship between inherent hazard factors, risk factors and hazardous event

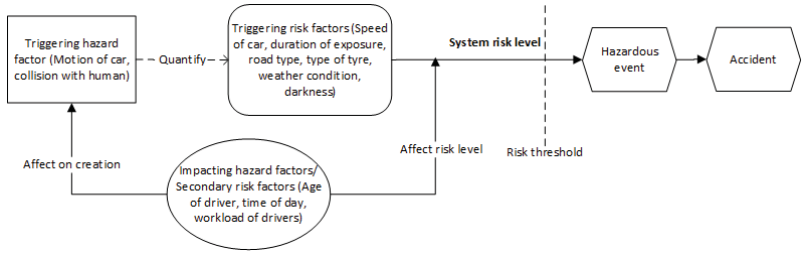


Figure 2: Relationship between inherent hazard factors, risk factors and the hazardous event, a person hit by a car

3.4. Hazardous event Boundary

A hazardous event is possible when a combination of inherent factors form a hazardous event boundary. If to create a hazardous event, three factors are necessary: flammability, congestion, and high pressure; if all three factors coexist with specific values without having any

safety measures in the system, then the hazardous event will occur. So, the probability and severity of the hazardous event is the function of all three factors.

4. INHERENT SAFETY AND INHERENTLY SAFER SYSTEM

4.1. Definition of Inherent safety

Inherent safety is the philosophy that reduces or modifies inherent hazard and risk factors present in a system, thereby reduces the probability or severity of a hazardous event in the system and prevents the occurrence of a hazardous event

Inherent safety works on reducing triggering inherent hazard factor and modifying inherent risk factors. The goal of inherent safety is to make a system hazardless. Theoretically, if we can eliminate all inherent hazard factors from the system, no initiating event will occur, and there will be no hazardous event. In practical cases, as we cannot eliminate them, we try to minimize them as much as possible to make the plant inherently safer. If a system possesses material hazards, the IS option eliminates those hazardous materials or substitutes them with a safer one. If elimination or substitution is not possible, another IS option is to modify the materials to make them less hazardous. Modification means we are changing the properties of a material, thus making it less hazardous.

An example could be to dilute a hazardous material with a less hazardous material. To ensure inherent safety, we need to reduce the inherent hazard factors as much as possible. An inherently safest design will not make any hazard, and an IS measure can never fail when it goes into operation. If we can assure a hundred per cent inherently safe plant, there will be no need for maintenance or inspection.

4.2. Difference between inherent, Passive and Active measures

IS measures are those measures which contribute to reducing or modifying inherent hazard and risk factor. Passive and active measures do not contribute to reduce or modify the hazards factor. We isolate the hazards and inherent risk factors by passive and active measures, so no hazardous events and accidents can occur. Isolation means putting a barrier between the hazard and inherent factors and other agents (can be machinery, human or other property), for example, putting insulation on an electric wire. Electric hazards are still there; we are only putting barriers between electric hazard and human being so they do not get harmed.

Another example can be a firewall. Fire hazards still exist. We are only putting barriers between fire and property. Passive and active measure principally do the same thing. The only difference is that active measures need engineering or human activation, while passive measures do not. Most hazards are related to generation and the existence of energy. In the case of reaction hazards, thermal and pressure energy are the inherent hazard factors. In the case of mechanical hazards, the generation of kinetic energy or the existence of energies is the inherent hazard factors. By adopting IS measures, we try to minimize inherent risk factors or ΔE (thermal energy produced in the reactor) or potential energy conversion from one type to another.

On the other hand, passive and active measures cannot minimise ΔE or potential energy conversion. A PSV transfers the ΔE to the environment, so the system or human's effect is limited. In the case of material hazard, they usually are the material properties, let us say $m_{p,}$ which is the inherent hazard factor. By inherent measures, we try to eliminate or modify those properties, m_p, so any hazardous event cannot occur by them, e.g. using a non-flammable material instead of flammable material.

4.2.1. Example of dust explosion

Dust explosion occurs due to the accumulation of powdered combustible material in a congested place, combined with high heat/energy and oxygen availability. Dust explosion depends on several factors:

Factor 1. The chemical property of material - combustibility
Factor 2. State of material – powder form
Factor 3. Presence of high energy – high heat/spark/ignition
Factor 4. Congestion
Factor 5. Oxidant
Factor 6. Concentration of material
Factor 7. Extensive property of material - quantity

These are inherent hazard factors. A hazardous event occurs when combinations of these factors present in the system form the hazardous event boundary.

Inherent safety works on modifying or reducing, or eliminating these factors. Inherent safety measures are:

- Selecting non-combustible material (eliminating factor 1- chemical properties of the material)
- Reducing combustibility of material (modifying factor 1- chemical properties of the material)
- Changing powder form of material by making it into a slurry (eliminating factor 2- state of material)
- Removing all energy sources from the system (eliminating factor 3 - the presence of high energy)
- Modifying layout to reducing congestion (modifying factor 4 - congestion)
- Modifying concentration or quantity, mixing inert solid with the powder (modifying factor 6)

An example of a passive measure is a venting panel. It does not change the material properties but transfers high-pressure energy from the system to the ambient to reduce pressure.

5. ACHIEVING AN INHERENTLY SAFER SYSTEM

To achieve IS of a system, two main strategies should be followed:

1. Reduction of the severity of triggering inherent risk factors
2. Modification of impacting inherent risk factors

5.1. Reducing the severity of triggering inherent risk factors

5.1.1. Proper selection

When selecting material or equipment, a safer material should be selected instead of a hazardous material or

equipment or reaction with different physical properties to reduce the severity of inherent risk factors. E.g. using a less volatile solvent with a higher flash point, substituting the reaction with less hazardous raw materials or intermediates, reducing inventories of hazardous material, choosing DC voltage.

5.1.2. Modification

Modification of material or equipment or reaction can reduce the severity of inherent risk factors. Modification can change the chemical/physical properties of material/equipment or change the system's condition. For example, dilute a material with natural solvent, decrease the reactivity, or make it of suitable shape and size. Modification of external properties will make it possible to carry the object easily. Modifying the reaction means the modification of reaction chemistry. Modification of the system can reduce the force or amplitude of something like refrigeration of pressured gas.

5.1.3. Minimization

As a strategy for reducing the severity of inherent hazard factors, when deselection or modification is not possible, less material or equipment should be used. If we use less material or execute a slight batch reaction, less energy will be produced. When we have two systems, they may possess several other hazards factors; their mitigation may need extra effort.

5.1.4. Transformation/Recycling

An IS measure is to reduce energy consumption in the overall system or reuse energy or recycle energy. Energy evolved from one machine can be stored and can be used for other purposes. The same principles go for the material. If a hazardous material is used in the system, recycling the material in several cases is possible, so the overall system's hazardous material consumption reduces.

5.1.5. Relocation/Rearrangement

Relocation of equipment can reduce congestion in the system. Rearrangement is related to facility layout. Also, it is expected that an IS system can tackle environmental occurrences, which are typical in any location. A structure can be subjected to high wind. The structure should have the capacity to bear such environmental occurrences. The system should have the capacity and options to carry out the activities safely. Vibrational energy produced by the machines used inside it or imposed by many populations should not hamper the structure.

5.1.6. Comprehension

Comprehensibility means that something is readily comprehended or understood. It includes making a user-friendly hardware device or software interface that is easy to use and difficult to learn or understand. Usability-related hazards often occur in the facility due to the complexity of a machine's working mechanisms, which is difficult for a worker to understand, or the tool is not designed correctly so that the user can use it easily. Many occupational accidents occur due to this.

5.2. Modification of the impacting inherent risk factors

Modification of impacting factors can be modifying the geometry or shape of equipment, as it affects the kinetic energy or modifying the internal part of a machine to reduce vibration, the noise produced by it. The component's physical properties, anthropometric dimensions, shapes, dimensions of contact surfaces can be modified to modify the component's movement or vibration and energy level.

6. Discussion

This paper presents the inherent safety principle defined by the inherent hazard and risk factors present in the system. Comparing the concept with Kletz (1985c), he describes four principles in this first proposal of inherent safety: intensification/ minimization, substitution, attenuation and simplification. Some other scientists reasonably identified the material hazards, reaction hazards and proposed inherent safety principles accordingly. Many scientists included error tolerance principles, making incorrect assembly impossible, making status clear, easing control, integrity, software, reliability, limitation of effects, etc., as IS principles (Heikkilä, 1999). The principle 'Limitation of effects' is confusing as we also use the passive and active measure to limit consequences. Therefore, there should be a distinction in defining the terms when applying them in different cases.

The minimization principle has often been highlighted in the literature as the potential approach to achieve inherent safety. As proposed by Kletz, one possible solution is that two storage tanks are preferable to one large tank. It has a theoretical basis also, as one large tank will hold high potential energy, so if the tank ruptures, kinetic energy will be higher than a smaller tank. However, two tanks will need more instrumentation, thus involves more mechanical hazard. So, when choosing the option between different alternatives, constraints should be carefully observed.

The present paper presents a concept of inherent safety explained by inherent hazard and risk factors. Inherent safety can be successfully achieved systematically by the identification of these factors. Relevant knowledge about inherent hazard and risk factors can be gained from a similar industry's accident database. Several factors may become responsible for creating a hazardous event, which may become identical for a similar plant type. The accident database will give knowledge about the kinds of accidents in the industry in the past. It should be checked whether relevant factors are still present in the system. After identifying the factors, relevant IS mitigation measures should be sought based on reducing the number of triggering inherent hazard factors or severity of triggering inherent risk factors and the modification of impacting inherent risk factors.

The strength of the proposed concept is that it can systematically identify inherent hazard and risk factors to find the causes of hazard. This systematic identification of factors helps the user to apply IS principle quickly and efficiently. Another strength of the concept is that it is applicable through the whole lifecycle of the plant. At the preliminary stage, when the opportunity to modify and

improve the design is most, the thinking about remedial material, reaction and system hazard will be most beneficial. Substitution of material or reaction, or system will not take extra effort and cost at this stage. At later stages of the project, the opportunity of elimination or substitution will be lesser and will demand a higher cost.

Another strength of the model is the ability to systematically compare two alternative designs more quickly in terms of inherent safety. Previously, scientists have compared alternative process routes where they mainly considered material hazard and reaction hazards. The present model is capable of doing a comparison considering all kinds of inherent hazard and risk factors. The present concept determines the inherent risk level of a system and compares the risk reduction by various measures by comparing the determined inherent risk level. Other risk analysis methods also identify the relevant risk factors and improve the design by modifying factors. However, in those methods, inherent and noninherent risk factors cannot be distinguished. So how much risk is reduced by inherent safety measures cannot be determined.

The drawback of the concept is that it is unacquaintance to the user. Users are entirely new to the concept. They may find it challenging to apply in practical cases. The method lacks the application of the concept for various practical cases.

7. Conclusion

Applying inherent safety measures and their integration at the early design stage is vital for any chemical or other process industry. In the paper, an approach to developing an inherently safer design based on identifying inherent hazard and risk factors has been proposed. Inherent safety measures are proposed based on inherent hazard and risk factors. Systematic classified identification of inherent hazard and risk factors can make it easier to find appropriate inherent safety measures considering their constraint. In the future, a model can be developed to quantify the interaction of various inherent risk factors and quantify the relationship between risk factors and the system's risk level. Identification of inherent risk factors for a specific application and finding IS measures can establish such a model.

8. Acknowledgement

The authors gratefully acknowledge the research council's financial support, Norway and DynSoL AS Norway through project no: 283861. We express our cordial gratitude toward the Engineering design team of DynSoL AS for their continuous research support. The contributions of project leader Kamrul Islam and project administrator Gisle Obrestad are also acknowledged.

9. References

ABEDI, P. & SHAHRIARI, M. 2005. Inherent safety evaluation in process plants—a comparison of methodologies. *Open Chemistry,* 3**,** 756-779.

ADE, N., KOIRALA, Y. & MANNAN, M. S. 2019. Towards an inherently safer bioprocessing industry: A review. *Journal of Loss Prevention in the Process Industries,* 60**,** 125-132.

AHMAD, S. I., HASHIM, H., HASSIM, M. H. & RASHID, R. 2019. Development of hazard prevention strategies for inherent safety assessment during early stage of process design. *Process Safety and Environmental Protection,* 121**,** 271-280.

BAHRI, Z., KLUE, R. A., TUCKER, J., NUGRAHA, R. & SMITH, J. D. 2009. ExxonMobil's Project Approach to Safety-Nobody Gets Hurt.

BERNECHEA, E. J. & VIGER, J. A. 2013. Design optimization of hazardous substance storage facilities to minimize project risk. *Safety Science,* 51**,** 49-62.

BP 2008. Inherently safer design. *Engineering technical practices.*

CHAN, I., ALWI, S. R. W., HASSIM, M. H., MANAN, Z. A. & KLEMEŠ, J. J. 2014. Heat exchanger network design considering inherent safety. *Energy Procedia,* 61**,** 2469-2473.

CHIAPPETTA, G., CLARIZIA, G. & DRIOLI, E. 2006. Analysis of safety aspects in a membrane reactor. *Desalination,* 193**,** 267-279.

COZZANI, V., TUGNOLI, A. & SALZANO, E. 2007. Prevention of domino effect: From active and passive strategies to inherently safer design. *Journal of Hazardous Materials,* 139**,** 209-219.

EDWARDS, D. W. & LAWRENCE, D. 1993. Assessing the inherent safety of chemical process routes: is there a relation between plant costs and inherent safety? *Process Safety and Environmental Protection,* 71**,** 252-258.

EINI, S., JAVIDI, M., SHAHHOSSEINI, H. R. & RASHTCHIAN, D. 2018. Inherently safer design of a reactor network system: A case study. *Journal of Loss Prevention in the Process Industries,* 51**,** 112-124.

ELJACK, F., KAZI, M. K. & KAZANTZI, V. 2019. Inherently safer design tool (i-SDT): A property-based risk quantification metric for inherently safer design during the early stage of process synthesis. *Journal of Loss Prevention in the Process Industries,* 57**,** 280-290.

ENGLUND, S. M. 1995. Inherently Safer Plants - Practical Applications. *Process Safety Progress,* 14**,** 63-70.

ETCHELLS, J. 2005. Process intensification - Safety pros and cons. *Process Saf. Environ. Protect.,* 83**,** 85-89.

FEI, Y., SUN, B., ZHANG, F., XU, W., SHI, N. & JIANG, J. 2018. Inherently safer reactors and procedures to prevent reaction runaway. *Chinese Journal of Chemical Engineering,* 26**,** 1252-1263.

GRIM, L., TILLEMA, D., CUTCHEN, S., WINGARD, M. & JOHNSON, A. 2015. CSB investigation of Chevron Richmond refinery pipe rupture and fire. *Process Safety Progress,* 34**,** 355-359.

GUPTA, J. 1997. Application of DOW's fire and explosion index hazard classification guide to process plants in the developing countries. *Journal of loss prevention in the process industries,* 10**,** 7-15.

GUPTA, J. P. & EDWARDS, D. W. 2002. Inherently safer design - Present and future. *Process Safety and Environmental Protection,* 80**,** 115-125.

HAMDAN, F. 2006. Structural strengthening of offshore topsides structures as part of explosion risk reduction methods. *HSE report rr489*.

HAME, W., KLEIN, D. & PIRK, H. 1980. Inherently Safe Air-Cooling for the Storage of Self-Heating Configurations of Radionuclides. *Atomkernenergie-Kerntechnik,* 35**,** 111-122.

HEIKKILÄ, A.-M. 1999. *Inherent safety in process plant design: an index-based approach*, VTT Technical Research Centre of Finland.
HENDERSHOT, D. C. 1997. Inherently safer chemical process design. *Journal of Loss Prevention in the Process Industries,* 10**,** 151-157.
HSE, U. 2007. *Offshore Health and Safety law* [Online]. Available: https://www.hse.gov.uk/offshore/law.htm [Accessed 15 march 2020].
IEC. 2020. *Internation Electrochemical Commission* [Online]. Available: https://www.iec.ch/ [Accessed 12 Nov 2020].
JAFARI, M. J., NOURAI, F., POUYAKIAN, M., TORABI, S. A., MIANDASHTI, M. & MOHAMMADI, H. 2018. Barriers to Adopting Inherently Safer Design Philosophy in Iran. *Process Safety Progress,* 37**,** 221-229.
KHAN, F. I. & AMYOTTE, P. R. 2003. How to make inherent safety practice a reality. *The Canadian Journal of Chemical Engineering,* 81**,** 2-16.
KHAN, F. I. & AMYOTTE, P. R. 2005. I2SI: a comprehensive quantitative tool for inherent safety and cost evaluation. *Journal of Loss Prevention in the Process Industries,* 18**,** 310-326.
KHAN, F. I., SADIQ, R. & AMYOTTE, P. R. 2003. Evaluation of available indices for inherently safer design options. *Process Safety Progress,* 22**,** 83-97.
KLETZ, T. 1978a. What You Dont Have, Cant Leak - Jubilee Lecture. *Chemistry & Industry***,** 287-292.
KLETZ, T. 1988. Plants Should Be Friendly. *Chemical Engineer-London***,** 35-35.
KLETZ, T. 1993. Major Hazards Onshore and Offshore - Manchester, 20-22 October 1992. *Journal of Loss Prevention in the Process Industries,* 6**,** 269-269.
KLETZ, T. A. 1977. Some Myths on Hazardous Materials. *Journal of Hazardous Materials,* 2**,** 1-10.
KLETZ, T. A. 1978b. Practical Applications of Hazard Analysis. *Chemical Engineering Progress,* 74**,** 47-53.
KLETZ, T. A. 1985a. Eliminating Potential Process Hazards. *Chemical Engineering,* 92**,** 48-68.
KLETZ, T. A. 1985b. Make Plants Inherently Safe. *Hydrocarbon Processing,* 64**,** 172-&.
KLETZ, T. A. 1985c. What Went Wrong - Case-Histories. *Hydrocarbon Processing,* 64**,** 81-83.
KLETZ, T. A. 1998. *Process plants: a handbook for inherently safer design,* Philadelphia, PA, Taylor & Francis.
KLETZ, T. A. 1999. *HAZOP and HAZAN: identifying and assessing process industry hazards*, IChemE.
KLETZ, T. A. 2004. Learning from experience. *Journal of hazardous materials,* 115**,** 1-8.
LUYBEN, W. L. & HENDERSHOT, D. C. 2004. Dynamic disadvantages of intensification in inherently safer process design. *Industrial & Engineering Chemistry Research,* 43**,** 384-396.
MANSFIELD, D. & CASSIDY, K. 1994. Inherently Safer Approaches to Plant-Design - the Benefits of an Inherently Safer Approach and How This Can Be Built into the Design Process. *Hazards Xii - European Advances in Process Safety***,** 285-299.
MANSFIELD, D., POULTER, L. & KLETZ, T. 1996. Improving inherent safety.
MEDINA-HERRERA, N., JIMENEZ-GUTIERREZ, A. & MANNAN, M. S. 2014. Development of inherently safer distillation systems. *Journal of Loss Prevention in the Process Industries,* 29**,** 225-239.
MIZUTA, Y. & NAKAGAWA, M. 2013. Development of Quantitative Hazard Analysis Method for Inherently Safer Chemical Processes. *Lp2013 - 14th Symposium on Loss Prevention and Safety Promotion in the Process Industries, Vols I and Ii,* 31**,** 247-252.
NORSOK, S. 2010. Risk and emergency preparedness assessment. *NORSOK Z-013*.
NTS 2001. Norsok Z-013
OHASHI, H., SATO, H., TACHIBANA, Y., KUNITOMI, K. & OGAWA, M. 2012. Concept of an Inherently-safe High Temperature Gas-cooled Reactor. *3rd International Conference on Advances in Nuclear Science and Engineering 2011 (Icanse 2011),* 1448**,** 50-58.
PALANIAPPAN, C., SRINIVASAN, R. & TAN, R. 2004. Selection of inherently safer process routes: a case study. *Chemical Engineering and Processing-Process Intensification,* 43**,** 641-647.
PASHA, M., ZAINI, D. & SHARIFF, A. M. 2017. Inherently safer design for heat exchanger network. *Journal of Loss Prevention in the Process Industries,* 48**,** 55-70.
PETROVIC, B. 2014. The Integral Inherently Safe Light Water Reactor. *Nuclear Engineering International,* 59**,** 26-29.
PIETERSEN, C. M. 1988. Analysis of the Lpg-Disaster in Mexico City. *Journal of Hazardous Materials,* 20**,** 85-107.
POHANISH, R. P. 2005. *HazMat data: for first response, transportation, storage, and security*, John Wiley & Sons.
QI, M., ZHU, J. Y., XU, J. M., ZHAO, D. F. & LIU, Y. 2019. Investigation of Inherently Safer Design Through Process Intensification: Novel Safety Assessment Methodology and Case Study in C-3-Alkyne Hydrogenation Distillation Process. *Industrial & Engineering Chemistry Research,* 58**,** 4866-4880.
RUSLI, R., SHARIFF, A. M. & KHAN, F. 2013. Evaluating hazard conflicts using inherently safer design concept. *Safety Science,* 53**,** 61-72.
SAMBETH, J. 1982. The Seveso Accident. *Chimia,* 36**,** 128-132.
SHRIVASTAVA, P. 1992. *Bhopal: Anatomy of a crisis*, Sage Publications Ltd.
STATOIL 2010. Guidelines for risk and emergency preparedness analysis. *Statoil GL 02822.*
STORNES, P. 2015. Risk influencing factors in maritime accidents: an exploratory statistical analysis of the Norwegian Maritime Authority incident database.
SUARDIN, J., MANNAN, M. S. & EL-HALWAGI, M. 2007. The integration of Dow's fire and explosion index (F&EI) into process design and optimization to achieve inherently safer design. *Journal of Loss Prevention in the Process Industries,* 20**,** 79-90.
SUMMERS, A. 2018. Inherently Safer Automation. *Process Safety Progress,* 37**,** 31-36.
TUGNOLI, A., KHAN, F., AMYOTTE, P. & COZZANI, V. 2008. Safety assessment in plant layout design using indexing approach: implementing inherent safety perspective. Part 2-Domino Hazard Index and case study. *J Hazard Mater,* 160**,** 110-21.
TYLER, B. 1985. Using the Mond Index to measure inherent hazards. *Process Safety Progress,* 4**,** 172-175.
ZAINI, D., PASHA, M. & KAURA, S. 2016. Inherently Safe Heat Exchanger Network Design by Consequence Based Analysis. *Proceeding of 4th International Conference on Process Engineering and Advanced Materials (Icpeam 2016),* 148**,** 908-915.

Paper IV

Sultana, Sharmin, and Stein Haugen. "Development of an inherent system safety index (ISSI) for ranking of chemical processes at the concept development stage." Journal of Hazardous Materials 421 (2022): 126590 (Sultana and Haugen, 2022)

Journal of Hazardous Materials 421 (2022) 126590

Contents lists available at ScienceDirect

Journal of Hazardous Materials

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

Research Paper

Development of an inherent system safety index (ISSI) for ranking of chemical processes at the concept development stage

Sharmin Sultana [a,b,*], Stein Haugen [a]

[a] Department of Marine Technology, Norwegian University of Science & Technology, NTNU, Norway
[b] Department of Research and Innovation, DynSoL AS, Norway

ARTICLE INFO

Editor: Dr. R Teresa

Keywords:
Inherent safety
System safety
Chemical industry
Process industry
Risk management

ABSTRACT

Inherently safer design is the most proactive approach to manage risk, as referred by scientists and experts. Researchers have adopted various methods in evaluating inherent safety indices like parameter-based indexing, risk-based indexing, consequence-based indexing, etc. However, the existing approaches have their limitations. The present paper focuses on establishing an inherent system safety index (ISSI) to evaluate inherently safer design during the concept development stage. The analysis starts by identifying a non-harmful system's inherent safety characteristics and related parameters. Four subindexes, determined from the non-harmful system's characteristics, are established using their relevant parameters. The safety of the chemical process system, the health of workers, and the environment's safety can be assured by selecting relevant parameters. Parameters are scored based on their deviation from the non-harmful condition. The sum of the deviations of the parameters gives the value of the inherent safety index. The case study looks at various routes of Methyl Methacrylate (MMA). According to the present case study, MMA production followed by Tertiary butyl alcohol is the safest route given health, safety, and environmental perspective. This approach helps overcome the limitation of parameter-based indexing, which arises from selecting predefined fixed parameters that become invalid in case of system variation or significant modification of the system. Besides, it considers the complexity and vulnerability that arises from the interaction of various factors|, which increase predetermined risk calculated at the design stage when the system is in operation. The subindices can be used individually if a focus is needed in *a* definite section of *a* system with *a* particular application or a smaller portion. This method is helpful for the industry in designing *a* safer plant considering the health, safety, and environmental perspective at the concept development stage.

1. Introduction

Inherently safer design (ISD) is a proactive approach to risk reduction (Amyotte and Khan, 2002). Risk reduction strategies fall into four types, inherent, passive, active, and procedural (CCPS, 2009). Inherently safer design strategy focuses on reducing hazard from the root, e.g., hazardous material or operations, rather than installing controlling systems (Heikkilä, 1999). This concept's application should start from the early design stage, unlike other strategies, which begin at the detailed design or commissioning stage (Shariff and Leong, 2009b). Along with its proactivity, this approach minimizes the cost of additional maintenance, energy, waste management, and pollution management and reduces the system's probability of failure (Abedi and Shahriari, 2005; Gupta and Edwards, 2002). Trevor Kletz, the pioneer of inherently safer design, proposed four main principles to achieve inherent safety (Kletz, 1978). These are intensification, modification, substitution, and simplification. Kletz, in his later works, introduced the concept of the friendly plant and included several other principles such as limitation of effects, making incorrect assembly impossible, tolerance, ease of control to make a plant more user-friendly (Kletz, 1988, 1989, 1990). Later several other researchers have worked on applying inherently safer design principles (Gowland, 1996; Ohashi et al., 2012; Theis and Askonas, 2013; Turney, 2001; Windhorst, 1995), establishing inherent safety guidelines (CCPS, 2009), finding conflicts in applying IS principles (Abidin et al., 2016; Hendershot, 1995; Rusli et al., 2013), etc.

With the expanded innovation of new technology and tools, achieving inherent safety by applying these principles in the chemical or process industry has become complex and complicated (Mannan et al.,

* Corresponding author at: Department of Marine Technology, Norwegian University of Science & Technology, NTNU, Norway.
E-mail address: sharmin.sultana@ntnu.no (S. Sultana).

https://doi.org/10.1016/j.jhazmat.2021.126590
Received 22 March 2021; Received in revised form 2 July 2021; Accepted 4 July 2021
Available online 10 July 2021

2015). Some recent accidents are the Richmond refinery accident of 2012, the BP (British Petroleum) Deepwater Horizon accident (Bly, 2011), and the BP Texas City refinery accident (Holmstrom et al., 2006). The casualties direct the attention that lack of proper application of inherent safety measures still exists. The design did not include enough Well integrity, which caused BP Deepwater Horizon Accident (Ingersoll et al., 2012). The Richmond Refinery accident could have been avoided by taking inherent safety measures at the plant design and operation stage, such as corrosion prevention of piping in an inherently safer way, ignition prevention, and avoiding hazardous activity (Grim et al., 2015). Adequate disposal equipment and inherent safety alternatives of disposal system such as flare could have prevented the BP Texas City refinery accident (Kaszniak, 2009). Kletz, in his latest literature (Vaughen and Kletz, 2012), expressed the opinion that the introduction of complex systems and digitization in the industry has introduced a gap in safety management that should be reduced. Industrial automation has introduced new challenges in process safety management (Kletz, 2009, 2012).

Researchers have been used various inherent safety evaluation methods to check the safety prospect of a design for a long time (Marchaterre et al., 1984, 1986; Tzanos et al., 1976; Waltar et al., 1985; Zobel, 1985). Established methods can be classified into six categories: consequence-based evaluation(Shariff and Zaini, 2010; Tugnoli et al., 2007), parameter-based indexing procedures, graphical assessment, risk-based evaluation, evaluation based on both safety and environmental prospects, and approaches based on optimization. In the consequence-based indexing approach, the potential of inherent safety is evaluated based on the estimated consequences for the system's specific design. Examples of such works are Dow's index (Murphy, 1995; AICHE, 1998), Mond index (Tyler, 1985; Lewis, 1979), I2SI (Khan and Amyotte, 2004), TORCAT (Shariff and Zaini, 2010), and the works of Etowa et al. (2002), Suardin (2006), Tugnoli et al. (2007), etc. Dow's and Mond's indexes have been used most widely in the industry for inherent safety evaluation. However, they are not usable in the early stage of process design, and the results are difficult to interpret (Rahman et al., 2005). These approaches cannot consider all aspects of inherently safer design, e.g., layout, the complex interaction, and require greater rigor, accuracy, and precision in quantifying the impact of safety measures on the values of hazard indices (Khan et al., 2001). The knowledge of I2SI can give the risk analyst confidence that the process is comparatively safer, considering the inherent safety perspective. The drawback of it is that it takes enormous effort and time to calculate all the steps. I2SI is not flexible enough when applied to different process design life cycles (Abedi and Shahriari, 2005). TORCAT can support the reduction of the severity of consequence by using inherent safety principles during the preliminary design stage. Modifying design is easy since TORCAT directly links process design simulation and the consequence model (Sharmin Sultana et al., 2020).

In parameter-based indexing methods, researchers select parameters that are relevant for specific applications. The final evaluation is done based on the condition of the parameters. This type of indexing method provides a direct relationship between various parameters and the occurrence of an accident (Athar et al., 2019). Prototype inherent safety index (PIIS) (Edwards and Lawrence, 1995) is the first work of parameter-based indexing. Heikkilä (1999) presents a simple weight-based inherent safety index (ISI) consisting of two sub-indices for chemical and process. The chemical sub-index considers chemical reactivity, the heat of reaction, chemical interaction, flammability, explosiveness, toxicity, and corrosiveness. Inventory, temperature, pressure, equipment safety, and safe process structure are considered in the process subindex. In the expert system (*i*Safe) method developed by Palaniappan et al. (2002), process routes are ranked based on selected parameters, and a graphical approach is designed for analyzing reaction networks. PIIS, ISI, and *i*Safe treat chemicals as individual components, not as a mixture. They cannot reflect the contribution of different elements in the mix (Shariff et al., 2012).

Leong and Shariff (2008) developed an inherent safety index module to determine the inherent safety level. The classification approach of Heikkilä (1999) is adopted for the ranking process. Based on the obtained indices, streams with unfavorable inherent safety levels are identified. In the process route index (PRI) developed by Leong and Shariff (2009), the level of explosiveness is considered a quantitative measure of the inherent safety level for selecting the process route. The level of explosiveness depends on fluid density, pressure, combustibility, mass heating value, and flammability. PRI can prioritize the inherently safest option among several process routes producing the same products. It considers chemicals in the processing system as a mixture. Changes in temperature and pressure on upper and lower flammability limits are also considered. The process stream index (PSI) (Shariff et al., 2012) is developed to compare and prioritize the level of individual stream's inherent safety level against overall streams. The method takes the particular parameter ratio for the selected stream against the simulation's average parameter values.

The ratio of parameters includes the ratio of heating value, pressure, density, and flammability limit. Using PSI, designers can prioritize the streams based on explosion potential and quickly identify the critical streams for improvement to avoid or minimize explosion hazards. Athar et al. (2018) established a chemical reactor inherent safety index. The index consists of three sub-indices: chemical, process, and reaction. The chemical sub-score is comprised of the scores for autoignition temperature, flammability, and explosiveness. The pressure and temperature of the process are considered in the process sub score. Three parameters are considered in the reaction sub-index — reaction parameter, reaction heat, and yield. A reaction parameter score is used to estimate the tendency to get a runaway reaction in a chemical reaction. Parameter-based methods have been widely used due to the early design stage's flexibility with less information available for process route selection (Srinivasan and Nhan, 2008). However, it has some shortcomings, such as subjective scaling and weighting factors. Parameters make a sudden jump in the score value at the sub-range boundaries, and it does not consider the interaction between different factors (Gupta and Edwards, 2003). Models are not flexible enough to incorporate additional available data. Parameters established for a specific type of industry may not be relevant for another sector. The parameter index-based approach does not help the user fully understand the hazards evolved in each process route as it does not discuss the exact cause of hazards.

Another problem is the dimensionality problem (Gupta and Edwards, 2003). Adding parameters of different dimensions like temperature (C), pressure (atm), inventory (t), toxicity (ppm), and comparing the summed value may become unacceptable scientifically from the chemical engineering point of view. Making the terms dimensionless and scoring parameters based on their hazard rating is time-consuming (Gupta and Edwards, 2003). It has been possible to overcome the shortcomings of the parameter-based indexing method, such as the dimensionality problem of adding parameters of different dimensions by applying graphical techniques as done in Gupta and Edwards' work. The graphic technique uses root cause analysis of accidents and compares selected parameters for inherent safety assessment. Gupta and Edwards (2003) work on a graphical approach for root cause analysis and comparison of selected parameters for inherent safety assessment. Ahmad et al. (2013) presented a visual procedure in designing an inherently safer design for both grass-root and retrofit cases in the petrochemical industry without including subjective scaling and a sudden jump in the score value. Graphical procedure visualizes the effect of parameters such as temperature, pressure, heat of reaction, process inventory, flammability, explosiveness, toxicity, and reactivity in the system using graphical way. The flexibility in parameter selection and subjective scaling has been removed in this work. In Tugnoli et al. (2012), accident scenarios are developed for the system. Relevant parameters are identified, which gives flexibility in parameter selection and establishes the logical relationship of parameters with accidents.

Index based on safety and environmental prospects consider

parameters that may impact health, safety, and environment (Hendershot, 1997). The inherent chemical process route index, proposed by Warnasooriya and Gunasekera (2017), considers potential toxicological impacts on the environment, the occupational health potential, and chemical process safety impact. The toxicological impact is selected as an environmental hazard. Chemical exposure due to fugitive emission is chosen as an occupational health hazard. Seven parameters are selected as chemical process safety impact, and subjective scaling is used for inherent safety evaluation. Seven parameters are inventory, chemical stability, temperature, pressure, flammability, and explosiveness. Inherent Benignness Indicator (Srinivasan and Nhan, 2008) is based on a multivariate approach using principal component analyses to compare process routes. Fifteen factors are considered related to health, safety, and environmental aspects. Various routes from health, safety, and environmental performances are also evaluated in Mimi Haryani and Wijayanuddin (2009). They considered flammability, explosiveness, toxic exposure, and reactivity for safety scoring. Material state, volitivity, and chronic toxicity are considered for the health index. For the environmental index, they regarded atmospheric toxicity, aquatic toxicity, and terrestrial toxicity.

Risk-based assessment techniques evaluate the risk inherent to a process owing to the chemical it uses and the process conditions (Eljack et al., 2019; Rathnayaka et al., 2014; Shariff and Leong, 2009a; Shariff and Zaini, 2013). However, the detailed procedures in finding probabilistic data and consequence determination take time and resources. The use of risk control measures, i.e., in RISI (Rathnayaka et al., 2014), may divert attention to more additional measures than inherent safety measures. The multi-objective optimization approach is adopted to overcome the conflicting objectives, e.g., increasing safety considering the cost (Eini et al., 2015; Lee et al., 2019; Suardin, 2006; Sugiyama et al., 2008; Vázquez et al., 2018).

The present paper establishes an inherent safety index for inherent safety evaluation at the chemical process's route and concept selection stage. To find a logical relationship between the selected parameters and predicted accidents, a non-harmful, inherently safer system is imagined. Relevant characteristics of such a non-harmful system are sought. Possible parameters are set which may affect the system to deviate from the non-harmful situation. This approach gives flexibility in the model to apply in a different kind of industry. Other types of hazards may become dominant for different applications. Searching characteristics of a non-harmful, inherently safer system will give flexibility in searching relevant parameters in IS evaluation model. Various scores are assigned based on the deviation of multiple parameters in the actual case from the non-harmful situation. Finding a deviation ratio removes the problem of dimensionality in determining the inherent safety index. Various parameters are also considered in the model, and penalty factors are assigned for various interactions. This consideration gives the logical reason that most of the accident occurs due to dangerous interaction of multiple parameters instead from the effect of a single parameter.

The present research only considers hazards related to the hazardous chemicals and processes used in the chemical industry, and the indices are proposed based on the identified hazards. Other types of hazards, e.g., geological or biological, are not considered here but can be included when considering another kind of plant. Section 2 of the paper discusses earlier work on various inherent safety index methods. Section 3 describes the detailed procedure of the proposed method for determining the inherent system safety index. The application of the index in a case study is described in Section 4. The case study evaluates the inherent safety of various routes for methyl methacrylate production and determines the best route. Section 5 presents the results obtained by applying the present method and compares them with previous works. This section also discusses the benefits and drawbacks of the present method. Section 6 presents a conclusion and describes possible future outcomes for extending the method.

2. Development of ISSI

2.1. Inherent risk and hazard factors

The establishment of the ISSI is based on the concept of inherent risk and hazard factors. The inherent safety characteristics are determined based on the system's possible hazards and risk factors. Hazard is the existence of factors that has the potential to cause harm to people, environment, or asset. Hazard factors are the properties, conditions, or causes that may cause harm. Hazard factors can be of two types: triggering hazard factors and impacting hazard factors. Triggering hazard factors are those factors which can directly contribute to a hazardous event. The presence of motion implies kinetic energy that can cause a hazardous event. Motion is, therefore, a triggering inherent hazard factor. Impacting hazard factors do not contribute to creating a hazardous event directly but affect the severity or probability of a hazardous event indirectly. The object's geometry affects the amount of kinetic energy and affects the related hazardous event's severity.

An inherent risk factor is the quantitative expression of the two types of hazard factors, triggering inherent hazards factors and impacting inherent hazard factors. Triggering inherent risk factors contribute to creating a hazardous event directly. In contrast, impacting inherent risk factors do not contribute to creating a hazardous event directly but may affect triggering inherent hazard factors or risk level in the system, thus changing the probability or severity of the hazardous event. The conceptualization of inherent risk factors assumes that the risk level (in terms of a quantitative measure) can be controlled by changing/ managing/ controlling the inherent risk factors.(Fig. 1).

2.2. Inherently safer system and real system

Fig. 2 shows an imaginary non-harmful, inherently safer system and a real system. An inherently safer system consists of four criteria — safe inflow, safe production, invulnerable, and simple. Design engineers always try to achieve these criteria as much as they can. Details of these four criteria are described in the next section.

2.3. Characteristics of an inherently safer system

Various types of risk factors evolved from various triggering and impacting hazard factors in the industry. Risk factors can be harmful physical or chemical properties of the material, for example, flammability, chemical instability, harmful reaction chemistry, harmful emission, or complexity. Complexity-related risk factors can be congestion, incomprehensibility. Moreover, the interaction of these various types of risk factors creates additional risks. The system should have such characteristics built-in to avoid all these risk factors or reduce these as little as possible to make an inherently safer system. The present method tries to identify the characteristics of a chemical process to avoid potential risk factors in the chemical process system. Various risk factors are identified from various earlier literature (Barbour et al., 1998; Brock, 1986; Greenberg et al., 1991; Keller and Associates, 2013; OSHA, 1983). The Present method tries to identify required inherent safety characteristics from system engineering concepts. After analyzing the inherent risk factors of a chemical process system, the authors determined that a chemical process system should have four characteristics to make an inherently safer system. The characteristics are safe inflow to the system, safe production in the system, less vulnerability, simplicity. The criteria are described in the following and summarized in Table 1.

2.3.1. Safe inflow to the system

To ensure safe material inflow, we need to select such raw material that is less hazardous. Inflow does not mean only the raw material of a reaction but refers to any material used for the whole system. So, inflow to the reactor system or any mechanical production system should be considered. If a process uses less hazardous material storage, the

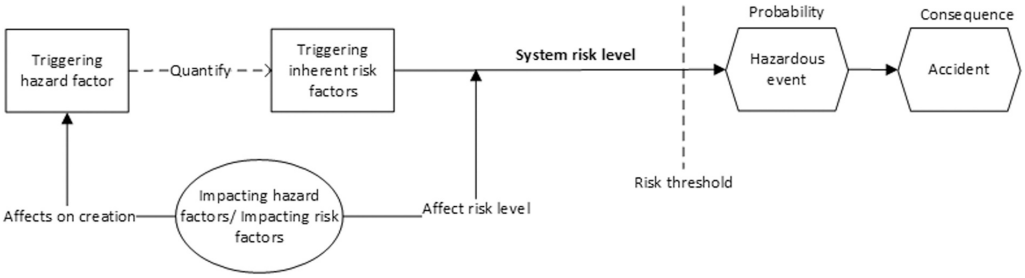


Fig. 1. Relationship between inherent hazard factors, risk factors, and hazardous event.

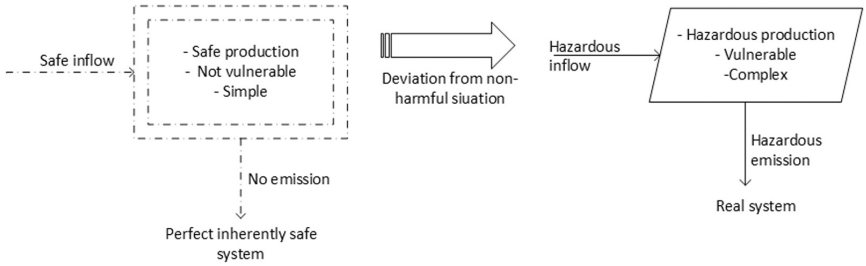


Fig. 2. Deviation from a non-harmful inherently safer system to the actual system.

Table 1
Overview characteristics, condition, and parameters of an inherently safer system.

Characteristics of the inherently safer system	Conditions related to the inherent safety	Inherent safety parameters
1. Safe inflow to the system	Safer material inflow	Chemical, physical, and external properties of the material (Flammability, chemical instability, corrosivity, viscosity, phase, quantity, or mass)
	Less energy consumption by the process and equipment	Energy consumptions by the process Energy consumption of the equipment
	Higher efficiency of the processes or equipment	Efficiency of equipment
2. Safe production of the system	Safer intermediate product or by-product	Chemical, physical, and external properties of the by-product and intermediate products
	Safer energy production	Heat of reaction
	Less production of waste material	Amount of waste material
	Less production of emission	Amount of greenhouse gas emission Amount in the form of CO_2, CO, steam, SO_2, etc.
3. Simple	Simpler processes and individual components and procedures	Process complexity parameters
4. Non-vulnerable	Safer process	Presence of unique hazardous process
	Compatible	Hazardous interaction between various parameters
	Safer process condition	Extreme hazardous condition

probability of leak or emission of hazardous material or the severity of the unwanted incident's consequence will be lower. Material's physical and chemical properties determine whether it will be hazardous or not. Physical properties are quantity, mass viscosity, toxicity, corrosivity. Flammability, instability, explosiveness, etc., are chemical properties (Brar, 2011). High energy consumption will create demand for a high level of electricity or other forms of energy. Since control of high energy will be difficult and hazardous (Klugmann-Radziemska, 2014), low energy consumption is an inherent safety characteristic. Energy requirements by the process and by individual pieces of equipment should be considered. Equipment with high efficiency will demand less energy, fuel, and material consumption. So if the equipment uses any hazardous material, high-efficiency equipment will consume less hazardous material in the long run (Clinton, 1994).

2.3.2. Safe production in the system

To ensure safe production in the system, we need to provide safer intermediate products and by-products and safer energy production. We need to select a reaction that does not produce any hazardous material or produces a meager amount of hazardous material as intermediate material or by-product. A machine that is crushing solids may create lots of dust material which is not desirable. Whether a product or intermediate material will be hazardous or not is determined by its properties, as have mentioned in Section 2.3.1. Dangerous energy evolution is the most common hazard in any industry. A reaction with a high heat of reaction needs extra control equipment to prevent other equipment and human from damage due to high heat (Crowl and Elwell, 2004). We have to select a process and reaction that produces less energy and has lower heat of reaction. If a process creates a higher amount of waste, it needs more control equipment to disburse the trash (Cheremisinoff and Cheremisinoff, 1995). Similarly, a process producing a higher amount of emission will need many redundant processes or equipment, which will increase the process risk (Xue et al., 2017). The amount of waste production and amount of emission is two inherent safety parameters that need to be considered in design selection.

2.3.3. Simple

This characteristic is applicable both at the components level and facility level. The characteristics include avoiding complexities of product, equipment, or information loading, simplifying the design by reducing operation steps, connections, congestion, and user-friendly processes. Some issues are thought to increase the complexity of a chemical process system. Examples of such matters are number of inputs and output streams, mixing steps, stages, critical changes in a route, changes of condition, state of process materials in the stream, the criticality of operations, number of equipment, type of equipment, number of unstable intermediates in a route (Song et al., 2018).

2.3.4. Less vulnerable

Vulnerability in a process system is created by the presence of a particular chemical process or extremeness of any hazardous properties of material or process. Vulnerability can also be created by the incompatibility of various process or system conditions evolved from the system's activity. Such incompatibility should be adequately identified. This inclusion is an essential condition as it is seen that despite having safer inflow in the system or relatively safer production in the system, these incompatibilities or conditions may increase the risk of a system to a large extent. There can evolve many such incompatibilities in a chemical process. The present research tries to identify some critical conditions possible to consider at the conceptual design stage. Conditions are as below:

- Presence of any unique hazardous process or chemical interaction; such as oxidation, hydrogenation, alkylation, etc. (Abedi and Shahriari, 2005)
- Incompatibility includes the presence of two hazardous conditions at the same time, such as highly toxic material at high pressure, highly toxic material with high vaporization, Highly volatile material at high pressure and temperature, etc. (Pohanish, 2017)
- The extremeness of any hazardous properties of the material or process, e.g., presence of highly flammable or toxic material in the system (Abedi and Shahriari, 2005)

2.4. Determination of ISSI

The ISSI comprises four subindexes: the inflow safety index, production safety index, complexity sub-index, and vulnerability sub-index.

$$ISSI = IFSSI + PSSI + CSI + VSI \tag{i}$$

Where IFSSI is the inflow safety subindex, PSSI is the production safety subindex, CSI is the complexity subindex, VSI is the vulnerability subindex.(i).

2.4.1. Inflow safety subindex (IFSSI)

For a chemical process, inflow safety refers to the safety of material that the system is taking per day or per hour. Along with the flow rate of material per hour or per day, storage inventory is also important. In the present method, inflow risk determines a property's deviation from a non-harmful situation. The inflow safety subindex is given as,

$$IFSSI = Dev_{IM} + Dev_{EC_{pr}} + Dev_{EQ} \tag{ii}$$

Where, Dev_{IM} is the deviation due to materials used in the inlet. $Dev_{EC_{pr}}$ is the deviation due to the energy consumption of the process. Dev_{EQ} is the deviation due to the energy consumption of the equipment. In the present paper, five material properties are considered to be most important for a chemical process. They are flammability, chemical instability, corrosiveness, toxicity, and quantity. There can be many other hazardous material properties. However, these properties can give quite a good indication of material safety (NFPA, 2017). Toxicity indicates a health hazard. Flammability and instability refer to chemical hazard which may become dangerous at high temperature and pressure. Corrosion is chosen as many minor- and large-scale accidents arise due to industrial corrosion in a chemical process.

$$Dev_{IM} = \frac{\sum_{i=1}^{m}\left(\left(Dev_{fl_i} + Dev_{CI_i} + Dev_{cor_i} + Dev_{tox_i}\right)/4\right)Dev_{Q_i}}{m} \tag{iii}$$

Here, Dev_{fl_i} is the deviation due to flammability of material' i′ in a process, Dev_{CI_i} is deviation due to chemical instability of material' i′ in a process, Dev_{cor_i} is deviation due to corrosiveness of material' i′ a process, $Dev(TX)_i$ is deviation due to toxicity of material' i′ in a process, Dev_{Q_i} is deviation due to the quantity of material' i′. m is the total number of materials in the inlet. Values of properties are determined, considering each component as individual components. The following equation should be used to evaluate the property of a mixture:

$$M = \sum y_i M_i \tag{v}$$

Where M_i is the property of individual component i, y_i is the mole percentage of a component in a stream (Perrot, 1998). Dev_{EQ} is determined by the following equation:

$$Dev_{EQ} = \frac{Dev_{EC_{eq}}.Dev_{eff_{eq}}}{N} \tag{iv}$$

EC_{eq} is energy consumption by individual equipment, eff_{eq} is the efficiency of individual equipment.

2.4.1.1. Determination of energy consumption of process. The following energy balance equation can be used to determine the energy requirement of a steady-state process:

$$\left\{\begin{matrix}\text{Energy input}\\ \text{with}\\ \text{input streams}\end{matrix}\right\} - \left\{\begin{matrix}\text{Energy output}\\ \text{with}\\ \text{output streams}\end{matrix}\right\} + \left\{\begin{matrix}\text{Energy}\\ \text{generation}\\ \text{within streams}\end{matrix}\right\} \pm \left\{\begin{matrix}\text{Energy}\\ \text{leaving or}\\ \text{added to system}\end{matrix}\right\} = 0 \tag{vi}$$

Mathematically,

$$(-\Delta H_{T_r}) + \sum_i n_i (H_T - H_{T_r})_i = \sum_j n_j (H_T - H_{T_r})_j + Q_{loss} + Q_{rec} \tag{vii}$$

Where n_i and n_j denote the number of reactants i and products j, respectively. $(-\Delta H_{T_r})$ represents the total reaction enthalpy occurring in the system at the reference temperature (T_r) (Sohn and Olivas-Martinez, 2014). For an exothermic reaction, this term is positive (i.e., energy input to the system). For overall endothermic reactions, it is negative. $(H_T - H_{T_r})_i$ is the addition of energy to the system in the form of the sensible heat of the reactants. $(H_T - H_{T_r})_j$ represents the energy removed from the system as sensible heat in the products. Q_{loss} is heat removed from the system to surroundings. Q_{rec} is the recoverable heat from the process. The energy requirement is found from the following equation (Sohn and Olivas-Martinez, 2014):

$$\text{Energy requirement} = (-\Delta H_{T_r}) + \sum_j n_j (H_T - H_{T_r})_j + Q_{loss} \tag{viii}$$

A chemical reaction's enthalpy change that occurs at constant pressure is called the heat of reaction. Standard enthalpy of reaction is calculated using standard enthalpy of formation of both reactants and products by using the below formula (Petrucci et al., 2010):

$$(-\Delta H_{T_r}) = \sum \vartheta_p \Delta H_f(\text{products}) - \sum \vartheta_r \Delta H_f(\text{reactants}) \tag{ix}$$

Where, ϑ_p is the stoichiometric coefficient of the product from the balanced reaction, ϑ_r is the stoichiometric coefficient of the reactants from the balanced reaction, ΔH_f is the enthalpy of formation for the

reactants or products in kJ/mol at the reaction temperature.

For a component which is solid at 25 °C, if the reaction temperature is above its boiling point, change of enthalpy is calculated by the following equation (Perrot, 1998):

$$\Delta H_f = \int_{298}^{T_m} C_p dT + \Delta H_{fus} + \int_{T_m}^{T_b} C_p dT + \Delta H_{vap} + \int_{T_b}^{T_r} C_p dT \quad (x)$$

$$C_p(T) = A + BT + CT^2 + DT^3 + ET^4 \quad (xi)$$

Where T_m is the melting point of a material, °C, T_b is the boiling point of the material, °C, T_r is reaction temperature, °C, ΔH_{fus} is the heat of fusion of material in kJ/mol, ΔH_{vap} is the heat of vaporization of material in kJ/mol, C_p is heat capacity in j/mol.K, a function of temperature, *A, B, C, D, E* are experimentally determined constants of a particular material and in a specific temperature range.

2.4.2. Production safety subindex (PSSI)

The following equation determines the production safety sub-index,

$$PSSI = \sum_{j=1}^{n} Dev_{PM_j} + Dev_{HR_j} + Dev_{w_j} + Dev_{em_j} \quad (xii)$$

$$Dev_{PM} = \frac{\sum_{i=1}^{m}\left(\left(Dev_{fl_i} + Dev_{Cl_i} + Dev_{cor_i} + Dev_{toxi}\right)/4\right)Dev_{Q_i}}{m} \quad (xiii)$$

Here, Dev_{PM} is a deviation due to material properties used in the process j. Dev_{HR_j} is deviation due to heat of reaction evolved in process j, Dev_{em_j} is deviation due to emission in the form of steam, vapor in process j, Dev_{w_j} is deviation due to the amount of waste material in process j. Deviations of material properties of chemicals are determined due to their four properties and inventory, as discussed in the earlier section. The flow rate is considered here to find the deviation of inventory. Feed and product rate for route steps are calculated using stochiometric factors, molecular weights of the chemicals present, and reaction step yields. The feed flow rate is calculated using the formula: Mass of reactant = Mass of desired product out /yield of reaction (Lawrence, 1996).

$$F_A = \frac{F_P * \vartheta_A * MW_A}{\vartheta_p * yr} \quad (xiv)$$

Here, F_A *is flowrate of a feed material A.* F_P *is the flowrate of product P.* ϑ_A *is stoichiometric coefficient of material A, found from the material balance equation.* ϑ_p *stoichiometric coefficient of product P.* MW_A *is the molecular weight of feed A.*

2.4.2.1. Determination of deviation of waste material. Previously there have been many kinds of research on the ranking of industries by their effluent in general (Ahmad et al., 2020; Pennington and Bare, 2001) or as a part of the inherently safer design (French et al., 1995, 1996; Mansfield et al., 1997). In the present method, to simplify the calculation, effluent ranking is done from the following equation:

$$Dev_{w_j} = \sum_{i=1}^{n} q_i DS_i \quad (xv)$$

Where, q_i is the quantity of chemical i in the effluent stream, n = total number of chemicals in the effluent stream, DS_i is the score of chemical i, in effluent stream, DSi of a chemical is determined based on its waste code which considers the following four properties: ignitable, corrosive, reactive, toxic (Baker et al., 1992; Rosenfeld and Feng, 2011). Deviation due to these four properties is determined using relevant tables and is averaged.

2.4.2.2. Determination of vapor emission. The amount of flammable vapor that will be produced immediately from a liquid at a temperature above its atmospheric boiling point can be calculated by the following equation (King, 2016):

$$Q_v = \frac{2Q_L C_P(T_1 - T_2)}{H_v} \quad (xvi)$$

Where, Q_v = mass of flammable vapour released (kg), Q_L = mass of liquid (kg), C_p = specific heat at $(T_1 + T_2)/2$ of liquid (kJ/kg.°C), T_1 = liquid temperature (°C), T_2 = atmospheric boiling point of liquid (°C), H_v = heat of vaporisation of liquid at T_2 (kJ/kg).

2.4.3. Complexity subindex (CSI)

One of the critical principles of inherent safety design is process simplification. If process configuration becomes complex, operators' and maintenance crews' control and prevention of errors also become more complex. The complexity of a process is ranked by selecting parameters that affect the control requirement of the process. This paper adopts the method proposed by Song et al. (2018) with several modifications to rank complexity. In the present method, the modified complexity index considers equipment complexity, the number of stages, the difficulty of processes, and the parameters specified by Song et al. (2018).

Parameters for process complexity considered fourteen parameters. Parameters are the total number of input streams, total number of the output stream, number of changes of condition, number of mixing steps, the total number of changes in the state of process materials, the total number of Flashing liquid, the total number of flashing inventory at ambient, number of time-critical operations, number of sequence-critical operation, number of critical changes of operations, equipment ranking, number of recycling of the process, number of stages, number of unstable intermediates. Number of the input stream, output stream, number of changes, mixing steps, changes in the state- this information can be obtained from the process flow diagram and the process description of each route. For equipment ranking following procedure is followed.

2.4.3.1. Ranking of equipment. This classification of equipment is done based on their hazard rating without considering their failure rate. Furnaces and flares are considered most hazardous as they are the most common ignition sources for any leaks (Instone, 1989; Planas-Cuchi et al., 1997) and more hazardous than reactors (AIChE and Dow, 1987). Compressors, high-pressure storage tanks are considered very unsafe as they contain moving parts (Marshall, 1987), they are subject to vibration, can release flammable gas in a case of failure (Heikkilä, 1999). Process drums, towers, heat exchangers, pumps containing flammable liquid are lower scores as they give lower loss statistics (Heikkilä, 1999; Instone, 1989; Mahoney, 1990). The safest equipment is equipment handling nontoxic and non-flammable material. Reactors pump above autoignition are more hazardous than process drum. A high-hazard reactor is more hazardous than a typical reactor (Heikkilä, 1999). (Table 2).

Table 2
Score for various types of equipment.

Equipment items	Hazard rating	Score
Equipment handling non-flammable and nontoxic material	Safest	0
Heat exchangers, pumps, towers, drums, atmospheric storage tank	Less hazardous	3
Air coolers, reactors, high hazard pumps	Moderately hazardous	5
Cooling tower, compressors, high hazard reactors, high-pressure tank, refrigerated storage tanks	Highly hazardous	7
Boilers, Furnaces, fired heaters, flares	Most hazardous (Instone, 1989)	10

2.4.4. Vulnerability subindex (VSI)

Chemical process systems may become vulnerable due to particular processes, the interaction of parameters, or extreme values of any specific parameters (Lawrence, 1996). Because in addition to stepwise deviation in risk level, extremism or interaction may vastly increase the risk level. Highly flammable or highly toxic material needs extra precaution and regular safety structure (Kletz, 1995; Lawrence, 1996). Yield is not a sensitive factor in system risk level. However, lower yield may lead to large recycles and large separation sections. Additional scores are assigned to consider these risk level changes, which are termed penalties. Vulnerability sub-index, $VSI = \sum penalties$. To assign penalty, a vulnerability scale is created (shown in Fig. 3), which is based on additional risk increment due to presence vulnerability factors. Risk increment can be increase in the probability of accident or increase in the severity of consequence if mishap happens.

Penalty and interpretation:

- 5: Very high-risk increment - the possibility of catastrophe if not controlled properly
- 4: High-risk increment - the potential of significant consequence if cannot be controlled
- 3: Elevated risk - need special attention to avoid mishap
- 2: Moderate risk increment - can be controlled with particular attention
- 1: Low-risk increment - can be controlled with ease

Following types of penalties are identified due to:

I. Special processes, which are especially vulnerable, need special control features, such as oxygen, hydrogenation, vice versa

Various penalty factors are assigned for unique processes as they need special control features. Examples of special operations are hydro-generation, hydrolysis, isomerization, and alkylations. They require special attention to handle the process (Heinemann, 1979). Processes that have a high toxic effect that is very harmful to the living creatures, such as halogenation (Safe, 1982), are given a score of 10. Moderately exothermic processes, such as alkylation, esterification (King, 2016), are assigned a penalty of 5. Mildly exothermic processes, e.g., hydrogenation, isomerization (King, 2016), are given a penalty of three.

II. Chemical interaction

Here, chemical interaction considers the unwanted reactions of process substances or the formation of intermediate products in the plant. They are also considered to introduce additional risk in the plant-based on reaction or intermediate products. Penalties for chemical interaction are assigned based on the EPA matrix (Hatayama, 1980) and hazard classification of chemical interaction (Heikkilä, 1999). The formation of highly toxic or flammable gas is given the highest penalty as they may cause the most hazardous accident, fire, and explosion. Formation of harmless, non-flammable gas is less harmful than other categories, hence given a penalty 1.

III. Interaction between various parameters that increases the risk level of a system

Penalty factors for interaction are determined based on possible interactions among various factors in the system. The risk level cannot be determined by simply summing up the risk score of parameters individually. If this was the case, we were lucky enough not to have a massive accident. In reality, the interaction between factors plays a significant role in the determination of risk level. Due to the interaction of various parameters, aggregated risk of a system may become huge, and accidents occur with high severity in that case (Lawrence, 1996). For example, among chemical properties, flammability, toxicity, and explosion are not internally correlated. Whereas for phase change, the value of these properties changes. The state of material plays a vital role in increasing risk due to these properties. In the presence of these properties, external properties such as quantity play significant value in the system. For a reaction, energy risk is controlled by the heat of the reaction. For lower yield and low reaction rate, residence time will be higher, and the system will be more exposed to high heat. Process parameters follow a similar trend in risk increment. If pressure increases, temperature also increases while the flow rate decreases. So, all the risk scores increase simultaneously. If the heat of the reaction increases, the temperature will increase in the system, thereby increasing the risk.

Any material which has hazardous intrinsic properties need special equipment and structure. Equipment or facility becomes unsafe if it handles hazardous material instead of a relatively safer material like water. A combination of chemical properties of material and energy sources is very hazardous. A small amount of energy source may create a severe accident in the presence of high chemical properties of the material's material and external physical properties. Flammability, chemical instability; these issues are dependent on temperature and pressure. If a system runs at a temperature in the material's flammability limit, care should reduce the interaction risk. Different scale of penalties is assigned based on assumed risk contribution in the system. Various types of interaction can be toxic material at high pressure with the possibility of flash off, high temperature with the possibility of flash off, and vice versa. Penalties are assigned based on the qualitative assessment of hazards from accident databases and case studies (Lawrence, 1996; Macdonald, 2004; Mannan and Lees, 2012; Stephanopoulos, 1984). If process temp is above a material's autoignition temp, it is most hazardous; hence the penalty score is 5. Process temp above flash point is less dangerous than earlier, therefore scored as 3.

IV. The extreme value of any specific parameter that increases the risk level of a system to a large extent

Extreme conditions of parameters include high flammability, high toxicity, high chemical instability, and vice versa. The extreme value of these parameters can increase the risk level to a vast amount. Penalty factors are assigned for extreme values of these parameters to consider the additional increase of risk level. Penalty score one per material is given when the deviation of the parameter is above 6. Operating temperature going above autoignition temp or boiling temp or flash point temp. Three types of penalty factors are assigned based on these three conditions. For lower yield, residence time will be higher; penalties are set for lower yields.

2.5. Determination of deviation from the imaginary non-harmful situation

The inherently safer design potential is determined by estimating the system's deviation of various parameters from the imaginary non-

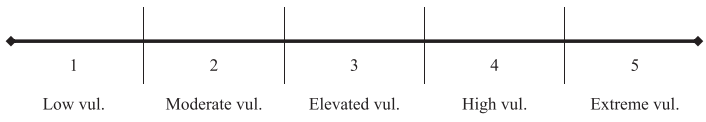


Fig. 3. Penalty score for vulnerability.

harmful situation. The deviation of each parameter is selected from predicted tables of deviations. Different deviational scores are given for multiple conditions. A minimum deviation is assigned as zero, and the highest deviation is set as 10. Various deviation scores are assigned according to their possibility of harm. For example, when giving a deviation score for the material property, flammability, zero is set for non-flammable material. Ten is assigned for highly flammable materials with a flashpoint below 0 °C. In the heat of reaction, a score of one is given for a neutrally thermal reaction, and a score of ten is assigned for a highly exothermic reaction, of which heat of reaction is more than 3000 kJ/kg. Various types of process equipment are also scored. Equipment handling non-flammable material is scored as 1, while fired heaters and flares are 10 (Instone, 1989; Planas-Cuchi et al., 1997). The deviation table for flammability is presented in Table 3. Deviational tables for other properties are shown in the Supporting Material.

2.5.1. Flammability

Flammability is how easily a material or a compound will burn or ignite, resulting in fire and combustion (ChemSafetyPro, 2021). The flammability of various materials is defined here by their flash point and boiling point. The flashpoint and boiling point of the mixture is calculated in the process simulator. The deviation score is assigned from the insight of GHS (global harmonization system) classification criteria (UN, 2003) and NFPA rating of hazardous materials (NFPA, 2017).

Other assumptions are as following:

- Materials, which has a flashpoint below 0 °C rapidly vaporize at atmospheric pressure and average temperatures, readily disperse in the air, and burn readily, are very flammable and most hazardous
- Liquid and solid, which has a flashpoint below 23 °C and initial boiling point below 35 °C, can easily ignite under normal temperature conditions, easily flammable, and secondly hazardous
- Materials, which has flashpoint which has below 23 °C and an initial boiling point above 35 °C, can ignite under normal temperature conditions, are less hazardous than the earlier category
- Materials which has a flash point above 23 °C and below 60 °C need to be lightly heated or to relatively high ambient temperatures to ignite them and are less flammable
- Materials which has a flash point above 60 °C and below 90 °C must be preheated before they ignite, are termed combustible
- Material with a flash point above 93 degrees Celsius is not be regarded as a flammable liquid or a hazardous chemical according to GHS classification criteria; hence here, the deviation is very close to the safest material
- Materials that do not burn are the safest in terms of flammability, such as water

2.6. Execution of procedures

Fig. 4 shows the work steps to determine the ISSI. It starts with the identification of the inherent safety characteristics of a relevant system.

Table 3
Various types of flammable material and related deviational score.

Flammability	Deviation score
Non-flammable	0
Less combustible (Flashpoint above 93 °C)	2
Combustible (Flashpoint at or above 60 °C, but below 93 °C)	3
Less flammable (flashpoint at or above 38 °C but below 60 °C)	5
Moderately flammable (flashpoint at or above 23 °C but below 38 °C)	6
Flammable (flash point below 23 °C and the boiling point at or above 38 °C)	7
Easily flammable (flash point below 23 °C and boiling point below 38 °C)	8
Very flammable (flash point below 0 °C)	10

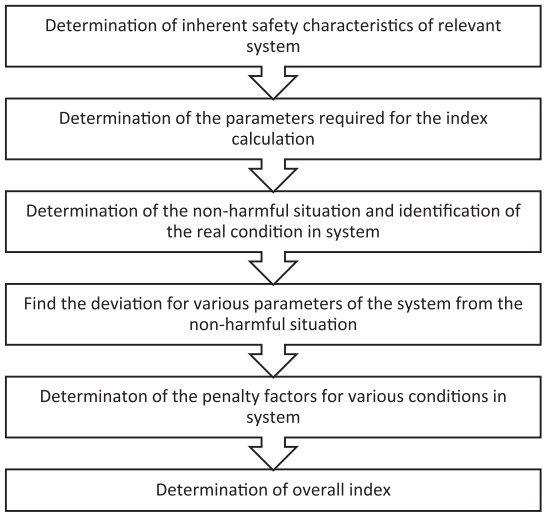


Fig. 4. Work steps to determine the ISSI.

At first, the inherent safety characteristic of a related system is identified for a non-harmful situation. Relevant parameters related to each characteristic are identified. The next task is to determine the values of each parameter in a non-harmful situation and an actual situation. The deviation of each parameter in an existing system is determined by finding its deviation from a non-harmful state. In addition to the deviation, various complexity factors are identified and scored. Various penalty factors are assigned after the evaluation of various interactions of parameters in the system. The overall index is calculated by using the equations earlier.

Fig. 5 shows the procedure of determining ISSI when comparing various design alternatives. Various alternatives are thought of at the beginning of the analysis. One needs to find inflow risk, production risk, complexity, and vulnerability index for each design alternative considering all process streams. Chemical properties and physical properties of material and reaction are collected from the chemical database. Energy consumption of equipment can be collected from the vendors. The streams involved in an alternative are distinguished to avoid repetitions of calculation. For each stream, material properties in the inlet stream and energy consumption by individual equipment are evaluated. Deviation due to each property is determined using deviation tables presented in Supplementary Material, and the inflow safety index is calculated using Eq. (ii). Properties of each material in the outlet stream of each equipment, emission, and amount of waste are evaluated. Production safety subindex is calculated using equation (xii). In the next step, various complexity factors that increase the system's complexity are sought, and the complexity subindex is calculated using factors described in Section 3.4.3. The vulnerability subindex is calculated from penalties due to various interactions present in the system. It is checked whether all the stream in a route is evaluated. When ISSI is calculated for an alternative, the analyst goes for another alternative and repeats the same process. Evaluation of all the alternatives indicates the completeness of the analysis.

3. Case study

3.1. Development of alternative routes

The present case study assesses various routes of the production process of Methyl Methacrylate (MMA). The assessed routes are the production of MMA by using Acetone Cyanohydrin (ACH); Ethylene via

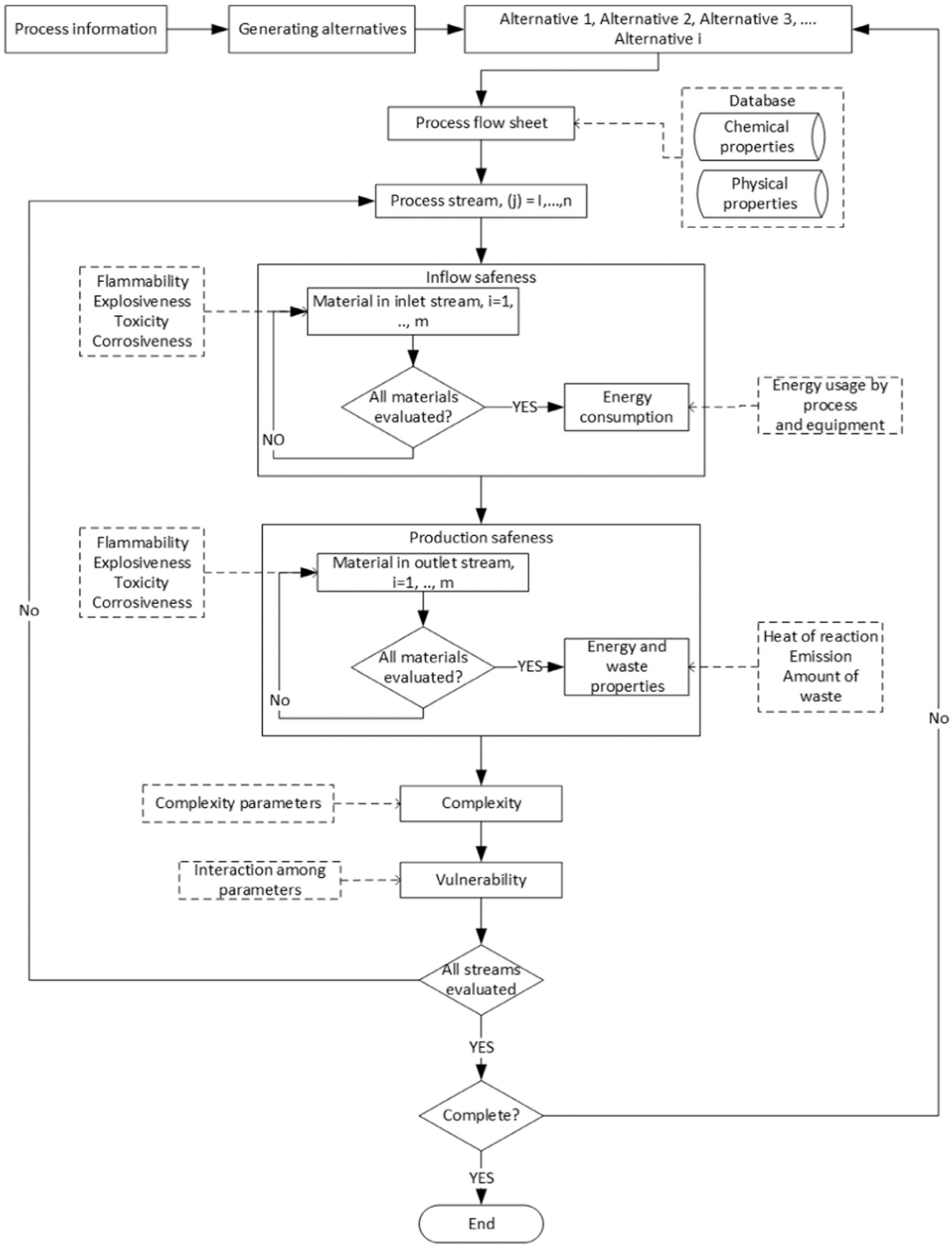


Fig. 5. Proposed framework for evaluating ISSI.

Propionaldehyde (C2/PA); Ethylene via Methyl-Propionate (C2/MP); Propylene (C3); Tertiary butyl alcohol (TBA), and Isobutene (iC4). Due to page limitation, ISSI calculation for only the ACH production route is shown here. An evaluation of ISSI for other routes is presented in the Supplementary Material.

3.2. Calculation of the indices for the ACH route

The acetone cyanohydrin process is the conventional process for MMA manufacture. Process flow of the route along with involved equipment and materials are identified in the process. The state of each parameter, reaction temperature, pressure, process changes, and any recycling is also investigated. Hydrogen cyanide is reacted with acetone to give acetone cyanohydrin (ACH). ACH is treated with sulfuric acid and heated to provide Methyl Acrylamide. The final step is the reaction of methyl acrylamide with methanol to produce MMA. The sulfuric acid is recovered from the Ammonium Bi-Sulphate by-product. A simplified process flow diagram is illustrated in Fig. 6.

3.3. Calculation of inflow safety subindex

Material flow in the storage and reactors is only considered to calculate the inflow safety subindex to simplify the calculation. First, it is identified which materials need to be stored. Materials that are supplied continuously pose some risk in their pipeline transportation. Pipeline transportation risk is not considered in the present case. Methane, ammonia, oxygen, acetone, and H2SO4 are stored temporarily for the ACH route. The chemical and physical properties of each involved material are collected from the relevant database. These properties often vary with the change of pressure and temperature. Due to the simplicity of the calculation, constant values of material are assumed irrespective of pressure and temperature change. The deviation of each parameter from the non-harmful condition is determined from the predefined tables shown in the Supporting Material. Inflow safety subindex is calculated using equation (ii). Supplementary Material contains detailed calculation processes. Deviation of material properties of these chemicals is determined due to their material properties and inventory. Inventory is calculated by using the following equation:

$$Storage\ inventory\ (kg) = 14\ days * daily\ flow\ rate\ (kg/day) \quad \text{(xvii)}$$

It is assumed that chemicals are stored for 14 days. Energy consumption by individual equipment, the efficiency of equipment, energy consumption by the process, calculation of waste materials is not considered in the case study due to lack of sufficient data and information.

3.4. Calculation of production safety subindex

In the present case study, the material production of the reactor is considered only to calculate the production safety subindex. The liquid will vaporize both from the reactor and storage. Deviation for vapor formation and heat production is determined. The heat of reaction is calculated using equation (*ix*). The vapor release rate is calculated using Eq. (xvi). While calculating feed and product flow rate for each step, yearly output from the plant is assumed as 50,000 t/yr, and the average operating hour of the plant is considered as 7500 h/yr. The actual recycling stream and recycle rate are not known. For simplicity, the feed and recycle stream is assumed as the feed stream. The flowrate of feed is calculated using equation (*xiv*).

3.5. Calculation of complexity and vulnerability subindex

Complexity parameters are found out from the PFD diagram (Fig. 6). ACH route has ten input streams, seven output streams, and three mixing steps. Seven reactors, two separators, two purifiers, and five storage tanks are used in the route. Overall equipment ranking is found out by considering the ranking of each equipment and number of equipment. Other complexity parameters are also found out from PFD and the information database. To calculate the vulnerability index after investing presence of special processes like oxidation or hydrogenation are investigated. Interactions of various parameters are sought for reactor and storage. Four interactions are found for the reactor. They are toxic material at high pressure, high toxicity with the possible flash off, high pressure with the possible flash off, and high temperature. One

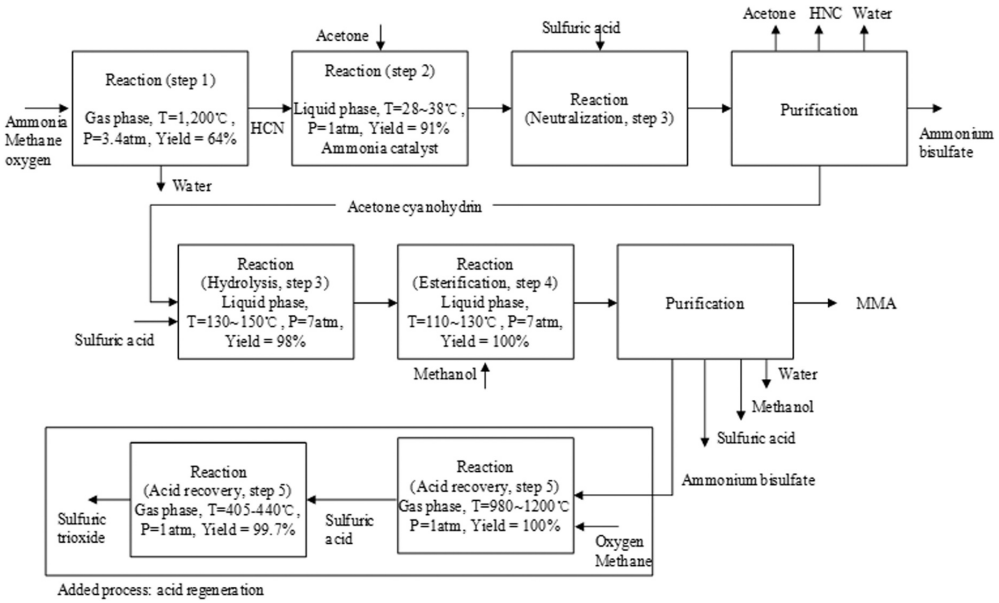


Fig. 6. MMA production by ACH route (Song et al., 2018).

interaction is found in storage which is high toxicity with the possible flash off. Four extreme parameters are investigated for storage and the reactor. They are very high flammability, very high instability, high toxicity, very high corrosiveness. Finally, the penalty is assigned for process temperature greater than autoignition temp or boiling point or flashpoint. All the penalties are summed to get the value of the vulnerability subindex.

3.6. Results

The calculated sub-indices and overall index by the present method are presented in Table 4.

4. Discussions

ACH route is most inherently unsafe, which is logical as it has the most significant number of stages, equipment, and streams, which increases its complexity and vulnerability. ACH route is worst considering its complexity and vulnerability, which is also apparent, as it has many unstable intermediates and many steps. C2-PA has the highest hazardous inflow to the route.

4.1. Comparison with earlier works

Various other researchers (Andraos, 2016; Anuradha et al., 2020; Gupta and Edwards, 2003; Mimi Haryani and Wijayanuddin, 2009; Song et al., 2018; Sugiyama et al., 2008) evaluated MMA production routes given inherent safety perspectives. The evaluation result is presented in Table 5. All of the methods show that TBA and iC4 are the most inherently safest methods among all others. The result varies because of different perspectives and selecting various parameters for those perspectives' s method. On a comparative analysis with PIIS, ISI, and iSafe, the authors evaluated the total index by adding scores for various parameters related to material and process. The complexity of the process and interaction of multiple parameters were not considered in those methods. Inherent benignness index uses principle component analysis to compare the routes.

The green metric method considers material consumption, energy consumption, material, and environmental impact. Each consumption and effect are determined quantitatively, and overall ranking is done based on the quantitative result of the assessment. In PRI, parameters which affect explosion accidents are considered only. In the work of Song et al. (2018), parameters are added without considering the difference in magnitude of hazard, the complexity of the procedure, or expert opinion. Fuzzy logic is used for chemical properties, process data, and chemical accident databases. The index considers the type of reaction and equipment parameter, process safety, complexity, operability,

Table 4
Determination of inherent system index (ISSI) and ranking by using the present method for various routes of MMA production.

Inherent safety sub-Indices	ACH route	C2-PA route	C2-MP route	C3 route	TBA route	iC4 route
Inflow safety sub index (IFSSI)	73.38	68.42	60.15	71.52	63.75	70.63
Production safety subindex (PSSI)	93.22	112.25	106.00	69.88	58.25	65.25
Complexity Sub index (CSI)	8.33	5.27	6.47	5.80	4.00	4.47
Vulnerability sub index (VSI)	132.56	104	130.25	110.25	46.5	60.75
ISSI index	307.48	289.93	302.86	257.45	172.50	201.09
Ranking	6	4	5	3	1	2

Table 5
Ranking of various routes of Methyl Methacrylate production by different inherent safety assessment methods.

Methods	Ranking					
	ACH route	C2-PA route	C2-MP route	C3 route	TBA route	iC4 route
Inherent safety performance index (Song et al., 2018)	5	3	4	6	1	2
PIIS (Song et al., 2018)	6	3	5	4	2	1
ISI (Song et al., 2018)	6	3	4	4	1	1
*i*Safe (Song et al., 2018)	6	2	5	4	3	1
Inherent benignness index (Srinivasan and Nhan, 2008)	6	2	3	5	1	4
Extended process route index (Athar et al., 2020)	–	3	4	–	1	2
PRI (Athar et al., 2020)	–	3	4	–	1	2
Green matric (Andraos, 2016)	5	3	4	6	2	1
SHE performance based (Mimi Haryani and Wijayanuddin, 2009)	4	6	1	5	3	2
Process route healthiness index (Hassim and Edwards, 2006)	5	3	4	6	1	2

and the chemical characteristics index and sub-indexes process characteristics. In the extended process route index (Athar et al., 2020), parameters for all equipment to reflect equipment characteristics are averaged for a process route compared with others. The Process Route Healthiness Index (PRHI) quantifies the health hazards that might arise from chemical processes. The PRHI is influenced by potential chemical releases and the concentration of airborne chemicals inhaled by workers that may impact their health.

The present method falls under the fifth category of the inherent safety evaluation methods described in the introduction, which considers health, safety, and environmental perspective. The method considers the chemical properties of material like flammability, chemical instability, and corrosiveness. Essential environmental aspects, toxicity, type of waste materials, and quantity of waste material are also considered. It also considers energy consumption and emission. Inherent safety methods are often subjected to having the limitation of considering a limited set of aspects. While considering inherent safety parameters developed from inherent safety characteristics, various relevant factors that should be given focus based on the system's type, nature, or location can be considered. This method considers materials as streams instead of individual material where it is relevant, unlike most hazardous material considered in other methods (Heikkilä, 1999). If only the most hazardous material is considered, the scope of opportunity to improve the design by substitution of hazardous materials becomes shorter.

4.2. Improvement in the calculation process

Adding parameters of different dimensions like temperature (°C), pressure (atm), inventory (t), toxicity (ppm), and comparing the summed value is unacceptable from the engineering point of view. Either we need to make the terms dimensionless or need the score parameters based on their hazard rating. Various deviation scores are assigned to parameters considering their hazard level to remove this dimensionality problem. Scored are assigned chiefly based on earlier guidelines (NFPA, 2017). Rest are given based on the qualitative judgment of possible hazard scenarios. Many accidents occur due to the complexity of the process, as the crew members and operators cannot handle it. The lack of incomprehensibility of the system is considered by determining fourteen

parameters related to it. Parameters consider the number of equipment, equipment complexity, the difficulty of the process, changes of state of the material, etc., which may induce additional risk.

4.3. The implication in overall risk consideration

Interaction of various parameters increases predetermined risk calculated at the design stage when the system is in operation, e.g., hazardous material in a reactor. Again, the extreme value of any parameter adds additional risk in the system, e.g., volatile material. The incapability to capture these interactions and considerations are often seen as the limitation of subjective scaling in parameter based indexing method (Gupta and Edwards, 2003). The reflection of vulnerability ensures that possible interactions between various risk factors are considered in the model. The selection of alternatives among many conflicting parameters is always challenging. This method can identify multiple, incompatible interactions of numerous parameters, which is crucial for any chemical process. Various penalties are assigned for temperature above autoignition temperature, boiling point temperature, or flashpoint temperature. Because the hazard of a subcooled liquid working at 350 °C is not the same as an overheated stream working at 400 °C, the risk is reflected by this penalizing. The unjustified measurement of the various parameters is balanced by assigning multiple penalties such as high pressure, high temperature, or high toxicity. Penalties are given due to high temperature and special vulnerable equipment.

4.4. Analysis with a specific focus

The subindices can be used individually if a focus in a particular section is needed, e.g., the production subindex can be calculated for various alternative designs to find the inherent safety perspective of a smaller portion of a plant such as a reactor. This method is flexible enough to analyze multiple systems, as it starts from identifying the inherent safety characteristics of the system and parameters related to those characteristics. This approach helps overcome the limitation of parameter-based indexing, which arises from selecting predefined fixed parameters that become invalid in case of system variation or significant modification of the system. This analysis will be helpful for the industry when designing a safer plant at the concept development stage.

Consideration of vulnerability and complexity has considered many factors, making it easier for engineers to modify the process accordingly. Modification is a crucial inherent safety principle. Although in practical cases, the application of this principle becomes very challenging. The detailed analysis of the present method will modify the system, reducing the pressure where material toxicity is high. If the parameter modification is not possible, the evaluated score will give design engineers caution in which factors should prioritize the detailed design stage. The method is easy to apply, not very time-consuming.

4.5. Limitation in scope

Although the present method reduces some of the limitations of earlier approaches, it still has some practical limitations. Hazards related to the chemical industry are only considered, and indices formulas are proposed based on that. There can be many other types of hazards, i.e., geological, biological depending on the application variability, which are not considered here. Material properties are affected by temperature and pressure. The value may also change due to other operations parameters in the system. A constant value of operating temperature is considered in the model. Considered operating temperature is the maximum average temperature that is obtained from field data of a similar factory. Some parameters are excluded from the established subindex, e.g., the scale of recycling fuel gas used, etc., to keep the method more straightforward due to the limitation of the scope of work. Although it has considered many interactions in any chemical process, many other interactions are not considered, e.g., ambient vapor pressure vs. threshold limit value and threshold limit value change for phase change. Risk level change due to many conflicting interactions of parameters are not considered, e.g., with the increase of the boiling point, the volatility decreases, thereby reduces the risk level. Again, if operating temperature increases, the risk level due to dispersion also increase. These effects are not considered here.

At the development process's route choice stage, it is impossible to say where intermediate storage will be placed or how much will be needed. Decisions about intermediate storage are made at the detailed design stage when the process flowsheet is available. In any case, provision for intermediate storage goes counter to the principle of an inherently safer design. Therefore, for the index, intermediate storage is left out of the inventory estimation. The distinction between long-time stored and transient chemicals is not considered. Five properties of materials are considered hazardous properties. Many other properties are considered, e.g., viscosity. While considering the complexity of equipment, ranking is performed based on numbers and type of equipment. The deviation score for various equipment is assigned based on their hazard rating in general, considering their type, type of material they handle, the maximum average temperature etc. Modern automated systems are equipped with many safety features. The features may reduce the complexity of the system, such as separate input/output module, devices with direct measurement possibility/failure on the specified state, simple graphical display, user-friendly human-machine interface, standard operating limit, enough margin in the alarm system, and distinguishable safety alarm from other alarms (Summers, 2018). Consideration of these features may give a different hazard rating from the established one here. The main focus in the present research is to identify parameters and their interaction that may affect risk level considerably at the concept development stage. Many aftereffects such as atmospheric stability and wind velocity on the leaked material's dispersion are not considered.

4.6. Possible future work

The present model can be used at different stages of process design. When detailed data such as equipment sizing, auxiliary equipment, etc., are available in the detailed design stage, the inherent safety level can be checked. The tool can be modified to consider all the relevant parameters. Other issues like layout, structural integrity are not included in the present model as it is developed focusing availability of parameters and data available at the concept development stage. The model can be modified to include these issues and to be used at later design stages. Future work can be done to increase the sophistication of the method and to remove the existing limitations. If the model can be linked with a process simulator, the processing options and safety evaluation can be accomplished simultaneously to detect unsafe conditions derived from changes in another unit. Future work should be directed toward applying the method in other chemical industries and other industrial applications.

5. Conclusion

A novel method to determine an inherent system safety index is presented in the paper. A case study is conducted to check the inherent safety perspective of various alternative Methyl Methacrylate production routes. After evaluating ISSI for various routes of MMA production, TBA is the safest route found from the analysis per the present method. The result shows variation with similar earlier approaches like SHE performance-based evaluation, Benignness index. The difference in perspective, the procedure of assessment, and selected parameters in those approaches are the causes for the variation.

Identification of the inherent safety characteristics of the system and identification of parameters related to those characteristics are the basis of the calculation of the present method. So, various types of systems can

be analyzed by using this single method. Evaluating inherent safety parameters derived from the inherent safety system's characteristics makes it possible to further extend the method in other industrial applications in the future. Deviation scores are assigned for various parameters based on the hazard rating of each parameter. This approach removes dimensionality in calculating various subindices, which was a limitation of the earlier parameter-based indexing methods. Interactions between various process parameters relevant to the chemical process industry are considered. The present research considers the interaction between different process parameters pertinent to the chemical process industry. The risk level of a system increases at the operational stage due to the interaction of various parameters. Various interactions are considered as 'vulnerability' parameters, and penalties are assigned for various vulnerabilities. Different complexity parameters are identified, which may decrease the comprehensibility of the system, thereby increasing the risk level, e.g., type of equipment, number of streams, etc. The approach will help the design engineers modify the process to make it inherently safer by identifying the specific factors more easily. However, these indices share general limitations, i.e., manual data extraction of process parameters. Hazards related to the chemical industry are only considered, and indices formulas are proposed based on that. Chemical instability is chosen to represent explosion and chemical reactivity hazards. Special cases like condensed phase runaway reactions are kept out of the scope of the present paper and can be included in the elaboration of the method in the future.

Various interactions and conflicting interactions are not considered. Future work can be done to increase the sophistication of the method. In the present work, the focus is given to technical issues only. Consideration of cost can be work on also in the future. If the model can be linked with a process simulator, the processing options and safety evaluation can be accomplished simultaneously to detect unsafe conditions derived from changes in another unit. Future work should be directed toward applying the method in other chemical industries and other industrial applications. The technique can be extended to use at later stages of process design. Layout, structural integrity, sizing of equipment, and other issues can be included in the model by including relevant parameters to assess inherent safety in the later stages.

CRediT authorship contribution statement

Sharmin Sultana: Conceptualization, Methodology, Software, Writing – original draft preparation, Visualization. **Stein Haugen:** Supervision, Writing – review & editing.

Declaration of Competing Interest

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

Acknowledgment

The authors gratefully acknowledge the financial supports from Research Council, Norway and DynSoL AS Norway through grant number 283861. We express our cordial gratitude toward the Engineering design team of DynSoL AS for their continuous support in executing the research's case study. The contribution of project leader Kamrul Islam and project administrator Gisle Obrestad is also acknowledged. The authors like to acknowledge their gratitude to anonymous reviewers for their valuable comments and advice.

Appendix A. Supporting information

Supplementary data associated with this article can be found in the online version at doi:10.1016/j.jhazmat.2021.126590.

References

Abedi, P., Shahriari, M., 2005. Inherent safety evaluation in process plants—A comparison of methodologies. Open Chem. 3, 756–779.
Abidin, M.Z., Rusli, R., Buang, A., Shariff, A.M., Khan, F.I., 2016. Resolving inherent safety conflict using quantitative and qualitative technique. J. Loss Prev. Process Ind. 44, 95–111.
Ahmad, S.I., Hashim, H., Hassim, M.H., Srinivasan, R. 2013. Safety Assessment Curve (SAC) for Inherent Safety Assessment in Petrochemical Industry. In: Proceedings of teh 16th International Conference on Process Integration, Modelling and Optimization for Energy Saving and Pollution Reduction *(Pres'13),* 35, 1267–1272.
Ahmad, S.I., Ho, W.S., Hassim, M.H., Elagroudy, S., Kohar, R.A.A., Bong, C.P.C., Hashim, H., Rashid, R., 2020. Development of quantitative SHE index for waste to energy technology selection. Energy 191, 116534.
AIChE, Dow, 1987. Fire & Explosion Index: Hazard Classification Guide. Amer Inst of Chemical Engineers.
AICHE, D.A., 1998. Dow's Chemical Exposure Index Guide. AIChE. Google Scholar, New York, USA.
Amyotte, P.R., Khan, F.I., 2002. An inherent safety framework for dust explosion prevention and mitigation. J. De Phys. Iv 12, 189–196.
Andraos, J., 2016. Complete green metrics evaluation of various routes to methyl methacrylate according to material and energy consumptions and environmental and safety impacts: test case from the chemical industry. ACS Sustain. Chem. Eng. 4, 312–323.
Anuradha, H., Gunasekera, M., Gunapala, O., 2020. Comparison of chemical routes based on inherent safety, health and environmental impacts of accidental and daily operational releases. Process Saf. Environ. Prot. 133, 358–368.
Athar, M., Shariff, A.M., Buang, A., Hermansyah, H., 2020. Equipment-based route index of inherent safety. Process Saf. Prog. 39.
Athar, M., Shariff, A.M., Buang, A., Shaikh, M.S., See, T.L., 2019. Inherent safety for sustainable process design of process piping at the preliminary design stage. J. Clean. Prod. 209, 1307–1318.
Athar, M., Zaidi, N.A.B., Shariff, A.M., Buang, A., Khan, M.I., 2018. Chemical reactor inherent safety index at preliminary design stage. IOP Conf. Ser.: Mater. Sci. Eng. 458, 012048.
Baker, R.D., Warren, J.L., Behmanesh, N., Allen, D.T., 1992. Management of hazardous waste in the United States. Hazard. Waste Hazard. Mater. 9, 37–59.
Barbour, A.K., Houghton, J.T., King, N.J., Matsui, S., Slater, D.H., Spiro, T.G., Taylor, D., Warner, F., Williams, D.R., Petts, J., 1998. Risk Assessment and Risk Management. Royal Society of Chemistry, Cambridge, Cambridge.
Bly, M., 2011. Deepwater Horizon Accident Investigation Report. Diane Publishing.
Brar, S.K., 2011. Hazardous Materials: Types, Risks and Control. Nova Science Publishers, Hauppauge, Hauppauge (Incorporated).
Brock, W.E., 1986. Safety & Health Guide for the Chemical Industry. Department of labor Washington DC occupational safety and health administration.
CCPS, 2009. Inherently Safer Chemical Processes: A Life Cycle Approach. John Wiley & Sons.
ChemSafetyPro. 2021. What is flammability? [Online]. Available: ⟨https://www.liquisearch.com/what_is_flammability⟩ [Accessed 2021].
Cheremisinoff, N.P., Cheremisinoff, P.N., 1995. Hazardous Materials and Waste Management: A Guide for the Professional Hazards Manager. Noyes Publications, Park Ridge, N.J.
Clinton, B., 1994. Technology for a Sustainable Future: A Framework for Action. US Government Printing Office, Washington, DC.
Crowl, D.A., Elwell, T.I., 2004. Identifying criteria to classify chemical mixtures as "highly hazardous" due to chemical reactivity. J. Loss Prev. Process Ind. 17, 279–289.
Edwards, Lawrence, 1995. Assessing the inherent safety of chemical process routes. Loss Prevention and Safety Promotion in the Process Industries, 1 and 2, B473–B482. WOS:A1995BE41U00097.
Eini, S., Abdolhamidzadeh, B., Reniers, G., Rashtchian, D., 2015. Optimization procedure to select an inherently safer design scheme. Process Saf. Environ. Prot. 93, 89–98.
Eljack, F., Kazi, M.K., Kazantzi, V., 2019. Inherently safer design tool (i-SDT): a property-based risk quantification metric for inherently safer design during the early stage of process synthesis. J. Loss Prev. Process Ind. 57, 280–290.
Etowa, C.B., Amyotte, P.R., Pegg, M.J., Khan, F.I., 2002. Quantification of inherent safety aspects of the Dow indices. J. Loss Prev. Process Ind. 15, 477–487.
French, R.W., Williams, D.D., Wixom, E.D. 1995. Inherent safety, health and environmental (SHE) reviews. *Lps 1995.* In: Proceedings of the 29th Annual Loss Prevention Symposium, 27–34.
French, R.W., Williams, D.D., Wixom, E.D., 1996. Inherent safety, health, and environmental (SHE) reviews. Process Saf. Prog. 15, 48–51.
Gowland, R., 1996. Applying inherently safer concepts to a phosgene plant acquisition. Process Saf. Prog. 15, 52–57.
Greenberg, H.R., Cramer, J.J., Stone, Webster Engineering, C., 1991. Risk Assessment and Risk Management for the Chemical Process Industry. Van Nostrand Reinhold, New York.
Grim, L., Tillema, D., Cutchen, S., Wingard, M., Johnson, A., 2015. CSB investigation of Chevron Richmond refinery pipe rupture and fire. Process Saf. Prog. 34, 355–359.
Gupta, J., Edwards, D.W., 2003. A simple graphical method for measuring inherent safety. J. Hazard. Mater. 104, 15–30.
Gupta, J.P., Edwards, D.W., 2002. Inherently safer design - present and future. Process Saf. Environ. Prot. 80, 115–125.
Hassim, M., Edwards, D., 2006. Development of a methodology for assessing inherent occupational health hazards. Process Saf. Environ. Prot. 84, 378–390.

Hatayama, H., 1980. A Method for Determining the Compatibility of Hazardous Wastes. Environmental Protection Agency, Office of Research and Development.
Heikkilä, A.-M., 1999. Inherent Safety in Process Plant Design: An Index-based Approach. VTT Technical Research Centre of Finland.
Heinemann, H. 1979. A Brief History of Industrial Catalysis.
Hendershot, D.C., 1995. Conflicts and decisions in the search for inherently safer process options. Process Saf. Prog. 14, 52–56.
Hendershot, D.C., 1997. Measuring inherent safety, health and environmental characteristics early in process development. Process Saf. Prog. 16, 78–79.
Holmstrom, D., Altamirano, F., Banks, J., Joseph, G., Kaszniak, M., Mackenzie, C., Shroff, R., Cohen, H., Wallace, S., 2006. CSB investigation of the explosions and fire at the BP Texas City refinery on March 23, 2005. Process Saf. Prog. 25, 345–349.
Ingersoll, C., Locke, R.M., Reavis, C., 2012. BP and the Deepwater Horizon Disaster of 2010. MIT Sloan School of Management (Case Study).
Instone, B., 1989. Losses in the hydrocarbon process industries. In: Proceedings of 6th International Symposium Loss Prevention and Safety Promotion in the Chemical Industries, Oslo, pp. 118–119.
Kaszniak, M. 2009. Examining Organizational and Safety Culture Causes of the BP Texas Cty Refinery Explosion.
Keller, J.J., Associates, I., 2013. OSHA Compliance Manual. J. J. Keller & Associates, Inc, Neenah, Neenah.
Khan, F.I., Amyotte, P.R., 2004. Integrated inherent safety index (I2SI): a tool for inherent safety evaluation. Process Saf. Prog. 23, 136–148.
Khan, Husain, Abbasi, 2001. Safety weighted hazard index (SWeHI): a new, user-friendly tool for swift yet comprehensive hazard identification and safety evaluation in chemical process industrie. Process Safety and Environmental Protection 79 (2), 65–80.
King, R., 2016. Safety in the Process Industries. Elsevier.
Kletz, T., 1978. What you dont have, cant leak - jubilee lecture. Chem. Ind. 287–292.
Kletz, T., 1988. Plants should be friendly. Chem. Eng. 35-35.
Kletz, T., 2012. The history of process safety. J. Loss Prev. Process Ind. 25, 763–765.
Kletz, T.A., 1989. Friendly plants. Chem. Eng. Prog. 85, 18–26.
Kletz, T.A., 1990. The need for friendly plants. J. Occup. Accid. 13, 3–13.
Kletz, T.A. 1995. Inherently safer design - The growth of an idea. *Lps 1995. In:* Proceedings of the 29th Annual Loss Prevention Symposium, 1–11.
Kletz, T.A., 2009. Don't just pass the parcel: accidents that would not have occurred if those involved had talked together. J. Loss Prev. Process Ind. 22, 667–671.
Klugmann-Radziemska, E., 2014. Environmental Impacts of Renewable Energy Technologies. Int Conf Environ Sci Technol. IPCBEE, Singapore, pp. 104–109.
Lawrence, D., 1996. Quantifying Inherent Safety of Chemical Process Routes (©). Duncan Lawrence.
Lee, Y., Kim, J., Ahmed, U., Kim, C., Lee, Y.W., 2019. Multi-objective optimization of organic rankine cycle (ORC) design considering exergy efficiency and inherent safety for LNG cold energy utilization. J. Loss Prev. Process Ind. 58, 90–101.
Leong, C.T., Shariff, A.M., 2008. Inherent safety index module (ISIM) to assess inherent safety level during preliminary design stage. Process Saf. Environ. Prot. 86, 113–119.
Leong, C.T., Shariff, A.M., 2009. Process route index (PRI) to assess level of explosiveness for inherent safety quantification. J. Loss Prev. Process Ind. 22, 216–221.
Lewis, D. The Mond Fire, Explosion and Toxicity Index-a Development of the Dow Index. In: Proceedings of the AIChE on Loss Prevention Symposium, New York, 1979.
Macdonald, D., 2004. Practical Industrial Safety, Risk Assessment and Shutdown Systems for Industry. Newnes, Amsterdam, Oxford.
Mahoney, D., 1990. Large Property Damage Losses in the Hydrocarbon-chemical Industries: A Thirty-year Review. M & M Protection Consultants.
Mannan, M.S., Sachdeva, S., Chen, H., Reyes Valdes, O., Liu, Y., Laboureur, D., 2015. Trends and challenges in process safety. AIChE J. 61, 3558–3569.
Mannan, S., Lees, F.P., 2012. Lee's loss prevention in the process industries: hazard identification, assessment, and control (ed). In: Mannan, Sam (Ed.), Loss Prevention in the Process Industries, fourth ed. Butterworth-Heinemann; Elsevier, Boston, Amsterdam.
Mansfield, D., Clark, J., Malmén, Y., Schabel, J., Rogers, R., Suokas, E., Turney, R., Ellis, G., Van Steen, J. & Verwoerd, M. 1997. The INSET Toolkit—Inherent SHE Evaluation Tool. AEA Technology/Eutech Engineering Solutions/INBUREX/Kemira Agro/TNO/VTT Manufacturing Technology, Risley (UK)/Winnington (UK)/Hamm (Germany)/Espoo (Finland)/Apeldoorn (Netherlands)/Tampere (Finland), version, 1.
Marchaterre, J., Sevy, R., Cahalan, J. 1986. Integral Fast Reactor Concept Inherent Safety Features.
Marchaterre, J., Sevy, R., Lancet, R., Mills, J., 1984. Key Asset-inherent Safety of LMFBR Pool Plant. Argonne National Lab.
Marshall, V.C. 1987. Major Chemical Hazards.
Mimi Haryani, H., Wijayanuddin, M. 2009. Screening Alternative Chemical Routes Based on Inherent Chemical Process Properties Data: Methyl Methacrylate Case Study.
Murphy, J. 1995. Dow's fire and explosion index - A risk reduction tool. 7th Ethylene Producers' Conference, Proceedings, 4, 252–270.
NFPA, 2017. NFPA 704, Standard System for the Identification of the Hazards of Materials for Emergency Response. National Fire Protection Association.
Ohashi, H., Sato, H., Tachibana, Y., Kunitomi, K. & Ogawa, M. 2012. Concept of an Inherently-safe High Temperature Gas-cooled Reactor. In: Proceedings of the 3rd International Conference on Advances in Nuclear Science and Engineering 2011 (Icanse 2011), 1448, pp. 50–58.
OSHA, 1983. General Industry: OSHA Safety and Health Standards (29 CFR 1910). OSHA, Washington, DC.
Palaniappan, C., Srinivasan, R., Tan, R., 2002. Expert system for the design of inherently safer processes. 1. Route selection stage. Ind. Eng. Chem. Res. 41, 6698–6710.
Pennington, D.W., Bare, J.C., 2001. Comparison of chemical screening and ranking approaches: The waste minimization prioritization tool versus toxic equivalency potentials. Risk Anal.: Off. Publ. Soc. Risk Anal. 21, 897–912, 897-897.
Perrot, P., 1998. A to Z of Thermodynamics. Oxford University Press on Demand.
Petrucci, R.H., Herring, F.G., Madura, J.D., 2010. General Chemistry: Principles and Modern Applications. Pearson Prentice Hall.
Planas-Cuchi, E., Montiel, H., Casal, J., 1997. A survey of the origin, type and consequences of fire accidents in process plants and in the transportation of hazardous materials. Process Saf. Environ. Prot. 75, 3–8.
Pohanish, R.P., 2017. Sittig's Handbook of Toxic and Hazardous Chemicals and Carcinogens. William Andrew.
Rahman, M., Heikkila, A.M., Hurme, M., 2005. Comparison of inherent safety indices in process concept evaluation. J. Loss Prev. Process Ind. 18, 327–334.
Rathnayaka, S., Khan, F., Amyotte, P., 2014. Risk-based process plant design considering inherent safety. Saf. Sci. 70, 438–464.
Rosenfeld, P.E., Feng, L., 2011. Risks of Hazardous Wastes. William Andrew.
Rusli, R., Shariff, A.M., Khan, F., 2013. Evaluating hazard conflicts using inherently safer design concept. Saf. Sci. 53, 61–72.
Safe, S., 1982. Halogenated hydrocarbons and aryl hydrocarbons identified in human tissues. Toxicol. Environ. Chem. 5, 153–165.
Shariff, A.M., Leong, C.T., 2009a. Inherent risk assessment-a new concept to evaluate risk in preliminary design stage. Process Saf. Environ. Prot. 87, 371–376.
Shariff, A.M., Leong, C.T., 2009b. Inherent risk assessment—A new concept to evaluate risk in preliminary design stage. Process Saf. Environ. Prot. 87, 371–376.
Shariff, A.M., Leong, C.T., Zaini, D., 2012. Using process stream index (PSI) to assess inherent safety level during preliminary design stage. Saf. Sci. 50, 1098–1103.
Shariff, A.M., Zaini, D., 2010. Toxic release consequence analysis tool (TORCAT) for inherently safer design plant. J. Hazard. Mater. 182, 394–402.
Shariff, A.M., Zaini, D., 2013. Inherent risk assessment methodology in preliminary design stage: a case study for toxic release. J. Loss Prev. Process Ind. 26, 605–613.
Sharmin Sultana, J.E. V., Jan Dahlsveen, Stein Haugen, 2020. Inherent safety assessment: current state of the art and why is still not effectively adopted by industry. 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, Italy. Research Publishing, Singapore.
Sohn, H., Olivas-Martinez, M., 2014. Methods for calculating energy requirements for processes in which a reactant is also a fuel: need for standardization. JOM 66, 1557–1564.
Song, D., Yoon, E.S., Jang, N., 2018. A framework and method for the assessment of inherent safety to enhance sustainability in conceptual chemical process design. J. Loss Prev. Process Ind. 54, 10–17.
Srinivasan, R., Nhan, N.T., 2008. A statistical approach for evaluating inherent benignness of chemical process routes in early design stages. Process Saf. Environ. Prot. 86, 163–174.
Stephanopoulos, G., 1984. Chemical Process Control. Prentice Hall, Englewood Cliffs, NJ.
Suardin, J.A., 2006. The Integration of Dow's Fire and Explosion Index into Process Design and Optimization to Achieve an Inherently Safer Design. Texas A&M University.
Sugiyama, H., Fischer, U., Hungerbühler, K., Hirao, M., 2008. Decision framework for chemical process design including different stages of environmental, health, and safety assessment. AIChE J. 54, 1037–1053.
Summers, A., 2018. Inherently safer automation. Process Saf. Prog. 37, 31–36.
Theis, A.E., Askonas, C.F., 2013. Inherently safer design concepts applied to laboratories. Process Saf. Prog. 32, 142–145.
Tugnoli, A., Cozzani, V., Landucci, G., 2007. A consequence based approach to the quantitative assessment of inherent safety. AIChE J. 53, 3171–3182.
Tugnoli, A., Landucci, G., Salzano, E., Cozzani, V., 2012. Supporting the selection of process and plant design options by inherent safety KPIs. J. Loss Prev. Process Ind. 25, 830–842.
Turney, R.D., 2001. Inherent Safety: What can be done to increase the use of the concept. HJ Pasman: Loss Prevention and Safety Promotion in the Process Industries-10th International Symposium, pp. 519–528.
Tyler, B., 1985. Using the Mond Index to measure inherent hazards. Process Saf. Prog. 4, 172–175.
Tzanos, C., Barthold, W., Bowers, C., Ferguson, D., Prohammer, F., Van Erp, J., 1976. Design-Related Inherent Safety Characteristics in large LMFBR Power Plants. Argonne National Lab., IL (USA).
UN, 2003. Globally Harmonized System of Classification and Labelling of Chemicals (GHS). United Nations, New York.
Vaughen, B.K., Kletz, T.A., 2012. Continuing our process safety management journey. Process Saf. Prog. 31, 337–342.
Vázquez, D., Ruiz-Femenia, R.N., Jiménez, L., Caballero, J.A., 2018. Multi-objective early design of complex distillation sequences considering economic and inherent safety criteria. Ind. Eng. Chem. Res. 57, 6992–7007.
Waltar, A.E., Padilla, A., Odell, L.D., Nguyen, D.H., Smith, D.E., Omberg, R.P., 1985. A perspective on the inherent safety of liquid-metal reactors. Trans. Am. Nucl. Soc. 49, 273–274.
Warnasooriya, S., Gunasekera, M.Y., 2017. Assessing inherent environmental, health and safety hazards in chemical process route selection. Process Saf. Environ. Prot. 105, 224–236.

Windhorst, J.C.A., 1995. Application of inherently safe design concepts, fitness for use and risk driven design process safety standards to an LPG project. Loss Prev. Saf. Promot. Process Ind. 1/2, B543–B554.

Xue, Y., Nie, L., Zhou, Z., Tian, H., Yan, J., Wu, X., Cheng, L., 2017. Historical and future emission of hazardous air pollutants (HAPs) from gas-fired combustion in Beijing, China. Environ. Sci. Pollut. Res. 24, 16946–16957.

Zobel, R. 1985. Computer Aided Compliance-A Tool to Increase the Inherent Safety of Vehicles. SAE Technical Paper.

Paper V

Sultana, Sharmin, and Stein Haugen. “An extended FRAM method to check the adequacy of safety barriers and to assess the safety of a socio-technical system.” Safety Science, 157.

Safety Science 157 (2023) 105930

Contents lists available at ScienceDirect

Safety Science

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

An extended FRAM method to check the adequacy of safety barriers and to assess the safety of a socio-technical system

Sharmin Sultana [a,b,*], Stein Haugen [a]

[a] Department of Marine Technology, Norwegian University of Science & Technology, Norway
[b] Department of Research and Innovation, DynSoL AS, Norway

A B S T R A C T

Safety barriers are used in the system to prevent unwanted events and accidents. Traditional approaches like fault tree or bow-tie method use linear accident models without considering complex interactions of failures of safety barriers. The present paper presents an extended FRAM model to identify required safety barriers and proposes a safety analysis method to predict the system's safety. The initial step of the method is to identify the necessary main and auxiliary functions to achieve the system goal. The later step is to determine the necessary safety functions to execute the main functions to achieve the system goal and to resist variability in performing the main and related auxiliary functions. A simple mathematical model is proposed to assess system safety based on the performance of existing barriers. The method is described with the help of a case study, the LNG ship-to-ship transfer process. The paper compares the extended FRAM method with other methods such as Bow-tie, FRAM-STPA, and Bayesian network. Analysis shows that FRAM can qualitatively, quantitatively, and dynamically assess system safety. The most vital point of FRAM lies in its capability of effective qualitative evaluation, which considers coupling between functions and related aspects, can be presented graphically, and future actions can be taken accordingly.

1. Introduction

Safety barrier management is crucial in reducing or maintaining control of a facility's process and system risk (Johansen and Rausand, 2015). Hardware (e.g., relief valves) or human (e.g., permission procedures), or a combination of both (e.g., manually actuated ESD system), can be used to create barriers. According to Petroleum Safety Authority Norway (PSA), the goal of barrier management is to develop and maintain barriers to the existing risk that can be managed by preventing or limiting the consequences of an unwanted incident (PSA, 2013).

Accidents are not single failures but rather complex situations of deviation of performance of several entities (Leveson, 2004). An increase in the dynamic complexity of the socio-technical system has made safety situations complicated. Accident scenarios for the presently used systems have become more challenging to describe. Examining potential scenarios and ways the system may behave rigorously is vital, ensuring that accident scenarios can be controlled and describing the scenario as realistically as possible. It is necessary to know the details of the accident's causes.

Most accidents in recent years are outcomes or the interaction of multiple aspects (e.g., technical, human, or organizational) present in socio-technical systems (Sawaragi, 2020). Traditional safety engineering approaches such as fault tree analysis, event tree analysis, failure mode and effect analysis cannot explain how multiple causes can lead to an accident (Thomas IV, 2013). Various system-based hazard analysis techniques have been developed to identify safety requirements in detail for complex socio-technical systems for solving the issue. Based on system-based accident modeling, proactive risk management strategies are developed, and the system is modified to prevent an accident (Rasmussen and Suedung, 2000).

In the conventional barrier approach, barrier performance is assumed constant, and risks are measured based on the static value (Zuijderduijn, 2000). In the ARAMIS (accidental risk assessment methodology for industries) EU project, coordinated by INERIS (French national institute for industrial environment and risks), bow-ties diagrams are used to identify significant accidents and check the sufficient safety functions. Each barrier's performance is evaluated based on response time, efficiency, and confidence level (Dianous and Fievez, 2006). The limitation of the bow-tie model is that it assumes accidents as a linear chain of events, which is not applicable when multiple causes are linked in complex ways. Another limitation of bow-ties is that barriers are not presented in a time or process following manner (Aust and Pons, 2020). Several works have been executed to overcome the limitation of the bow-tie. One such work is the work of Khakzad et al. (2013). They mapped the bow-tie model into the Bayesian network.

In the work of Bensaci et al. (2020), bow-tie and STPA (System Theoric Process Analysis) are applied together for detailed hazard

* Corresponding author.

https://doi.org/10.1016/j.ssci.2022.105930
Received 19 April 2022; Received in revised form 21 July 2022; Accepted 12 September 2022
Available online 21 September 2022

identification and evaluation of risk scenarios. STPA is based on the STAMP (System Theoric Accident Model and Processes) accident model for dealing safety in complex socio-technical systems (Leveson, 2011). In STAMP, the system is decomposed into components into controllers and controller targets. STAMP contains input, output function, control, and human and functional behavior. Pre-condition, resources, and time elements are absent in STAMP (Qiao et al., 2019). STPA establishes a control structure and identifies potential unsafe control actions and their causes. It can extract various hazardous events caused by system interactions. The analysis is suitable for the automated system due to its control structures. It is a purely qualitative method.

The barrier performance degradation rate is dynamic and needs continual monitoring and processing of real-time data (Paltrinieri et al., 2015). Dynamic barrier management (DBM) infers barrier status in near real-time and evaluates the impact on risk level. However, the DBM framework is challenging to implement and requires further development to clarify steps. In the work of Hosseinniaa et al. (2019), the authors propose a three-phase process for the DBM framework: screening, re-evaluation, and implementation. During the screening phase, a design baseline is established for barrier performance monitoring and to know the effect on risk level, then tracking the changes affecting the validity of the baseline profile. This step can be further divided into a context model, categorization of system changes, and gap analysis. Several steps are followed, such as a risk barometer to establish the context model. Three significant changes include the change in context, knowledge, and conditions. The effects of identified changes are reviewed by performing gap analysis on barrier elements, barrier function, and system performance and assessing the impact on risk level.

FRAM is used to derive potential accident scenarios. It focuses more on the understanding of interactions in complex socio-technical systems. FRAM evaluates the concept of stochastic resonance. It can be applied by identifying functions with detailed information about how something is done, characterizing the variability of the functions, interpreting possible couplings, and providing suggestions to manage the unexpected variability (Tian et al., 2016). FRAM has been widely applied in various fields, such as healthcare (Patriarca et al., 2018), aviation (Herrera et al., 2010, Rutkowska and Krzyżanowski, 2018, Tian and Caponecchia, 2020), maritime (Lee and Chung, 2018, Lee et al., 2020, Qiao et al., 2022, Salihoglu and Beşikçi, 2021), railway (Belmonte et al., 2011, Yue et al., 2020), environment and process industry.

In the work of Huang et al. (2019), the author used FRAM in the railway transportation system. FRAM provides an understanding of interactions and emergence phenomena in complex socio-technical systems. It focuses on behavioral changes rather than human failures, which helps managers comprehensively understand security. In the failure caused by functional resonance, when the output of the function changes, the reasons for the changes can be analyzed and found, and the most effective improvement suggestions according to the resonance situation can be obtained. FRAM shows that accidents can be prevented by controlling the output of functions or adding barrier measures to functions, which focuses more on reducing unsafe disposable behavior. According to the authors, FRAM is a better method to reduce the probability of accidents effectively and quickly in a short period.

In the work of Rutkowska and Krzyżanowski (2018), the FRAM method is used to examine air traffic control (ATC) service, a complex socio-technical system, to determine complex interactions in the daily operation of the system. It is seen that the FRAM model can facilitate the monitoring and controlling of the variable performance of ATC work. It also describes how the system components' functions can resonate and create hazards due to, for example, the lack of data updates, which, if undetected in time, can lead to accidents or serious incidents. The model can analyze the workflow and provide the means to conduct risk analysis and prevent risk by corrective activities. Based on the created model, it is possible to take further steps. It would allow for a more detailed model expansion to supplement the ATC services' coordination and control transfer processes. The created model for coordinating and transferring control over aircraft may be utilized to confirm or refine the ATC services' operational instructions and perform their revision. Gad et al. (2022) apply FRAM to identify financial risk factors concerning relevant stakeholders before the construction phase. The work proved the applicability of FRAM in performing financial risk analysis to support the project management team during the construction project phases.

Anvarifar et al. (2017) applied a customized FRAM method to compare various design alternatives for multifunctional flood defense. While the customized FRAM approach has only been applied to a single specific scenario and system problem in this research, the proposed method seems promising for identifying the threats and opportunities associated with the design alternatives of multifunctional flood defenses during the conceptual design phase. The method provides a qualitative tool for a broader view, analysis, and visualization of many imaginable internal and external changes to the system, including various types of human, technical, and environmental interactions. Furthermore, it provides a unified terminology and convenient framework to be used by the developers of multifunctional flood defenses from different domains. Additionally, the results can be used to identify the possibilities for appropriately increasing the system's flexibility to respond to various human and environmentally induced unexpected events. Overall, FRAM can serve as a valuable complement to the reliability analysis methods for enriching the risk analysis of multifunctional flood defenses. The proposed method, however, suffers limitations and needs further development. Guidelines are required for developing the scenarios and how much detail to include in the analysis.

Vieira and Saurin (2018) applied FRAM for a case of an environmental disaster that occurred in Brazil. FRAM made it possible to derive the system's outputs encountered in the disaster moment along with the magnitude of these outputs in each function. Actions are proposed to prevent similar disasters, and a discussion regarding the utility of this method in socio-ecological systems is presented. In the work of Seo et al. (2021), the authors applied three methods, AcciMap, STAMP, and FRAM, to analyze a fire accident. Although the approaches to finding the cause of an accident in these three methods are different, the results are almost similar. AcciMap and STAMP models are hierarchical. They play complementary roles in analyzing each component of the system. FRAM is more effective for analytics centered on human and organizational functions.

FRAM has been combined with other methods like STPA RAG to address industrial problems (De Linhares, 2021; Toda et al., 2018). FRAM combines accident causation analysis and a taxonomy model to identify and analyze operational risk (Li et al., 2019). FRAM can be used as a method to propose indicators where there is a high probability of performance variability. Sequentially timed events plotting method (STEP) and FRAM model are addressed in the work of Herrera and Woltjer (2010). STEP illustrates the event sequence showing the relationship between allocated authorities and the time sequence. One advantage of FRAM is that it helps the analyst look beyond the specific time sequence and failure under analysis. It provides a more comprehensive understanding and more effective learning of a possible accident (Herrera and Woltjer, 2010). It is possible to instantiate accident scenarios occurring in a limited time interval by FRAM.

Albery et al. (2016) executed a comparative risk assessment with various tools like work as imagined vs. work as done, risk matrix, and FRAM. The assessment showed that the comparative risk matrix focuses on specific hazards and their controls in isolation. The evaluation of work imagined vs. work as done also identifies local hazards and indicates hazard prevention. However, for a modern complex system to include variability in the overall structure and to gain comprehensive knowledge about the state of other related systems, a comprehensive tool is needed, which is possible by FRAM. FRAM assesses barrier management for offshore drilling in the work of Pezeshki (2020). Their case study demonstrates the method's potential barrier management in the strategy development phase. A potential hazard is identified first. Reactive barrier functions were integrated using the FRAM model.

Scenarios that can increase variability are controlled. The scenario analysis shows that variability is increased in human functionality and not the technical elements of the system. One great strength of FRAM is that it can be considered an iterative barrier strategy procedure in barrier management (Herrera et al., 2010).

Despite many recent works; only a few cover the quantitative evaluation of FRAM. A semi-quantitative FRAM is proposed by Patriarca et al. (2017) based on Monte Carlo simulation to assess performance variability in a complex system. The work summarizes various aspects like the complexity level of the system, organization condition, system condition, and disruption effect. In case of variability increases due to external conditions, functional resonance affects other functions, which makes other potential sources of variables. Human organizational factors such as communication coordination play an essential role in each function's execution. Yang (2020) proposed a formula consisting of safety entropy, functional conformability, and system complexity to check the spontaneity of the safety state-changing process.

Davatgar et al. (2020) use a mathematical model to visualize the link between changes in risk influencing factors and their effect on every part of the system. The Katz centrality algorithm assigns the initial edge weight of corresponding background functions. A dynamic FRAM graph model is presented for assessing operational risks arising from maintenance. The dynamic FRAM graph model systematically manages the couplings and functional variability information to lessen the effort needed to identify possible resonance propagations. RIFs related to functional variability are defined to evaluate the functional variability score in background and foreground functions to capture this concept. This approach captures the effect of changes within the system. It systematically prioritizes critical stages and interactions during maintenance work through graph topological analysis by considering Katz's centrality and Edge betweenness algorithms in two different operational situations.

An extended FRAM method is applied in the present paper to check the adequacy of safety barriers for a process system used in the chemical and petroleum industry, where technologies are well understood. Safety barriers refer to actions, procedures, resources, or equipment to keep the system in place or achieve the system's goal. In the case of these process systems, failure of barriers will create unwanted accidents and events. There can be many types of variability in other systems, e.g., geographical territory, financial organization, and public administration. These types of systems will require distinct types of measures to prevent system degradation. The method to find out system degradation relevant to those systems and measures to resist those degradations is not considered while developing the method and conducting the paper's case study. The method described in the paper is developed considering risk and safety barriers applicable to a chemical or petrochemical process system.

FRAM is adopted considering its potentiality to evaluate interactions of various factors in the system and dynamic behaviors suitable for the present socio-technical system. In previous works of FRAM, the hazard identification method is not well established, and a mathematical model for risk assessment is scarce. Further challenges exist regarding barriers, indicators, and re-design of functions and organizing data during the early stage of accident investigation (Herrera and Woltjer, 2010). Present work focuses on further study in this direction. FRAM method is extended to include a quantitative assessment tool to predict system status based on performance evaluation of existing barrier functions. The adequacy of barriers is also checked with the Bayesian network, FRAM-STPA, and Bow tie method. A qualitative comparison is made among them.

The case study chosen here (the LNG STS system) has already been studied in the academy and industry (Aneziris et al., 2021; Fan et al., 2022; Wu et al., 2021; De Andrade Melani et al., 2014). However, the reason for analysis again is that from the analysis of a known system, the effectiveness of the study's method will be visible. It will be clear whether the industry will be benefitted from the method, whether methods can improve the system's safety, and how companies will be helped. The paper is arranged as follows: In the first section, the necessity and background of the research are explained. The second section describes the analysis methods executed in the paper and their procedure. The third section shows the execution of the method with a case study. LNG (liquified natural gas) ship-to-ship transfer is chosen for the case study as it involves excellent interaction of humans, technology, and organization. The following section discusses the insight obtained from the analysis and concludes.

2. Method

The present extended FRAM method can be used for a system's hazard analysis or safety analysis. The method is implemented in several steps. The first four are related to functions and their execution for achieving the system's goal. Rest two are related to identifying required safety barriers that will ensure the implementation of main functions if they can be executed appropriately. As a result, the system's goal will be achieved precisely and timely.

2.1. Step 1:Identifying functions and aspects related to the goal of the system

The method's foremost step is to determine the system's goal precisely. For a chemical plant, the goal is to produce chemicals in a predetermined quantity on time in a safe manner. Related goals are to produce chemicals 'in predetermined quantity, 'on time', and 'safe execution'. The system's main function is identified based on the goal and understanding of how the system operates. Any distinction is not made for the type of entity performing the task (technical, human, or organizational) during identification. Description of function should provide necessary information to achieve the specified goal. Functions related directly to system goals are defined as 'main functions'. Additional functions are required for the execution of the main function. They are termed 'auxiliary functions'. In Fig. 1, F3 is the main function related to the system's goal. F1 and F2 are auxiliary functions, meaning the F3 function will be executed after F1 and F2. In other words, the F3 function cannot be performed without performing the F1 and F2 functions.

Next, aspects are defined related to each identified function. Five aspects are conceptualized similarly to typical FRAM (Patriarca et al., 2020). Output (O) results from the function related to a goal or related to the next target task. The final output function can be getting the desired product for a chemical process. Input (I) starts the function or preliminary task for the output function. Input for 'getting desired produce' can be 'inserting raw materials into the reactor'. Pre-condition (P) are conditions that must be fulfilled for executing the function. For example, the operator must be present during operation, or ambient conditions should fulfill the predefined criteria to start the function. Resources (R) are needed for carrying the function, for example, equipment, instruments, utility, procedure, or guidelines (Patriarca et al., 2020).

Control is anything that helps to monitor or control the function. It can be local operators carrying the task or supervisors or management monitoring it. Time (T) is the determinant related to the duration of the output function. It can be specified as a target, and functions can be set accordingly. For example, if 3 min target is set to finish the task, the time is 3 min. Other input functions and required pre-conditions can be set accordingly. If the task duration takes longer, the goal is not fulfilled (Patriarca et al., 2020).

2.2. Step 2: Determining interaction between functions

The interaction between functions, including aspects of each function, can be determined to visualize coupling between upstream and downstream functions (Erik, 2017). Description of each aspect of a function points to one or more other functions since the aspect of that

function must be provided by the performance of those related functions. The FRAM diagram (Fig. 1) depicts the system's functions and interaction paths. Upstream is linked with downstream aspects like input, pre-condition, time, control, or resource. For example, both function 'F1′ and 'F2′ are downstream functions of F3. Resource of F3 is linked to the output of function' Resources arrives'. The pre-condition of function F3 is related to 'Task to meet PC'. Control of function F3 is related to the 'Control arrives' function. This coupling is determined by looking at the system as a whole, functions that should be performed to achieve the goal, characteristics of how integrated to achieve the goal, and how one element influences other functions or aspects.

2.3. Step 3: Identify variability in functions and aspects

This step determines what variability can happen in the function and aspects. Variability is determined by the potential abnormal performance of each function. Possible performance of a function falls into four categories: Precise, Omitted, Imprecise, Too late/stopped in the middle. Descriptions are as follows:

i) Precise: A function is performed as required in time and with expected precision
ii) Omitted: A required function is not performed at all
iii) Imprecise: A required function is performed insufficiently with unacceptable precision
iv) Too late/stopped in the middle: A required function is performed late or stopped in the middle

The variability of a function is highly related to other aspects (input, pre-condition, resources, and control) of the same function. Any variation in the performance of these aspects will affect the output function and, thereby, goal-related o it. The performance of the five aspects is mirrored in the performance of the upstream function. When the variability of multiple functions resonates, the outcome of upstream functions varies unexpectedly. The variability of a single function is usually inadequate alone to cause an accident. When the variability of several functions resonates, variability might exceed the standard limit and result in an incident (Hollnagel and Goteman, 2004). The variability of aspects and the possible effect on the output are described in Table 1. The insufficient output of function F3 can be caused by variability in its four aspects or F1 or F2 (Fig. 1).

2.4. Step 4: Identify resonance effects or causal factors of the variability

This step is to identify the root causes of the variability. Root causes of variability are related to other functions. Route cause is the resonance effect of variability of other downstream functions of a specified function (De Carvalho, 2011). Route cause is identified considering each type of variability. In Fig. 1, a variability of F3 can be that F3 is not executed. Causal factors can be input function (F1 or F2) not executed or Precondition does not meet as 'task to meet PC' not executed. Other causal factors can be the absence of resources or control. The execution time of function F3 will be late if the execution of function 'arrival of resource' is late or the implementation of function 'arrival of control 'is late (Fig. 1). In this way, a deterioration in function performance or variability in function performance is developed from the resonance effect of variability of other related functions or aspects.

2.5. Step 5: Establish required safety functions to prevent variability of functions and related aspects

This step determines the safety functions that need to be implemented in order to avoid variability of functions and their aspects. Safety functions are related to the safe execution of the main and auxiliary functions. Safety functions are determined by considering the variability's resonance effect or route cause. Each safety function represents a safety barrier. The system's safety deteriorates when related safety functions cannot be executed in time. Safety functions are allocated considering three conditions:

i) Safety function to nullify the reason for abnormal state of aspects which resonates from downstream functions and aspects
ii) Safety function to nullify the reason for the abnormal state due to external effects

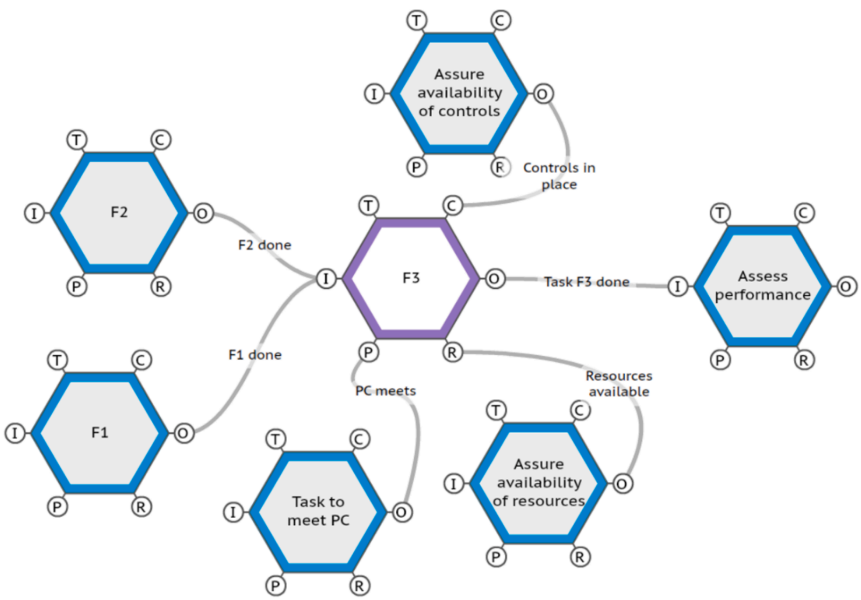


Fig. 1. Coupling between functions in FRAM.

Table 1
Variability of aspects and possible output variability.

Aspect	Variability of the aspect	Description	Possible output variability
Input	Omitted	Not executed at all	Not executed
	Imprecise	Executed with deficiency	Imprecise/Not executed
Pre-condition	Omitted	Pre-condition could not be met	Imprecise/not executed
	Imprecise	Pre-condition met with deficiency	Imprecise/not executed
	Late/stopped in the middle	Pre-condition met later	Later/not executed
Resource	Omitted	Resource is absent	Imprecise/not executed
	Imprecise	The resource is present with a deficiency	Later/imprecise/not executed
	Late/stopped in the middle	The resource is present later	Later/imprecise/not executed
Control	Omitted	Control is absent	Imprecise/not executed
	Imprecise	Control is present with deficiency	Imprecise/not executed
	Late/stopped in the middle	Control is present later	Later/imprecise/not executed
Time	Too short	Function execution took a longer time	imprecise
	Too late	Function execution took a longer time	Later
	Stopped in middle	Function interrupted in the middle	Later/imprecise/not executed

iii) Safety function for mitigation of the abnormal state that affects upstream functions

There can be various safety functions to prevent the variabilities. All possible functions should be considered to establish redundancy of safety. For example, there can be multiple safety functions like sf1 or sf2, or sf3 To execute function F3 precisely (Fig. 2). All should be considered here. After determining the safety function, each aspect related to the safety function is defined. Achievement of the goal depends on the state of output functions, which relies on the state of the input function, pre-condition, resources, control, and time. These states rely on the execution of safety functions. If one safety function cannot be executed, it will affect others. Safety functions should be managed properly to ensure the avoidance of hazards.

2.6. Step 6: Identify safety performance indicators

The result of FRAM analysis, obtained from step 5 of the method (Section 2.5), can be utilized to determine a system's performance indicator. Safety barrier performance indicators are determined by translating safety functions into quantifiable quantities. While translating, required input functions, resources, or controls related to safety functions are converted into measurable attributes used as indicators. These are leading indicators indicating potential safety actions taken by the facility. Lagging indicators can be developed using the system's variability of function and aspect. It indicates performance variability observed in the facility in a specified period. An example of translation is shown in Table 2.

2.7. Step 7: Assessment of safety performance of the system

The system consists of multiple levels. The performance of a target function depends on the contribution of various aspects from different levels. This level distinction is based on the execution sequence, not on time. Because functions at the various levels need to be executed simultaneously, it depends on the necessity of the system in Fig. 2, F3 is the main target function that is directly related to the goal. Resources R, Control C, Pre-condition PC, and Input function I are connected to this function at level i. Each aspect is related to other required functions at level i-1. Each function at i-1 is related to some other functions at level i-2.

Two factors assess the system's safety performance: aspect weight

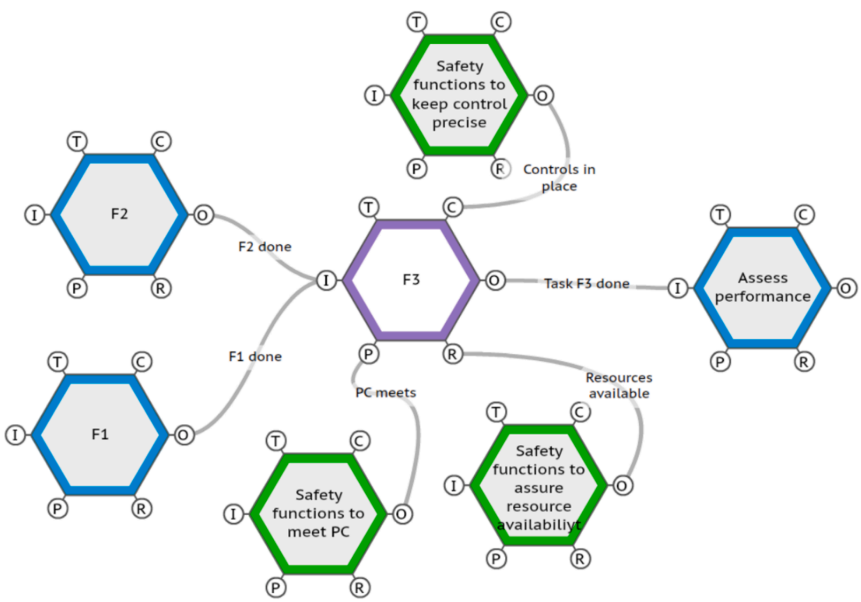


Fig. 2. Safety function for executing a target function in FRAM.

Table 2
Development of performance indicators from aspects of safety functions in FRAM.

Safety function	Related aspects	Related functions/ attributes	Performance indicators
Safety function S1	Output function OS1		
	Input function IS1	Actions are taken starting IS1	The number of the actions taken starts with IS1, quality of actions
	Pre-condition PCS1	Actions were taken to fulfill PCS1	Number of actions taken to fulfill PCS1, quality of actions
	Control CS1	Actions were taken to maintain control of CS1	Number of actions taken to maintain control of CS1, quality of actions
	Resources RS1	Actions were taken to assure resource availability RS1	Number of actions taken to assure resource availability RS1, quality of actions
Safety function S2	Output function OS1		
	Input function IS2	Actions are taken to start IS2	Number of actions taken start IS2, quality of actions
	Pre-condition PCS2	Actions were taken to fulfill PCS2	Number of actions taken to fulfill PCS2, quality of actions
	Control CS2	Actions were taken to maintain control of CS2	Number of actions taken to maintain control of CS2, quality of actions
	Resources RS2	Actions were taken to assure resource availability RS2	Number of actions taken to assure resource availability RS2, quality of actions

and deviation. Weight is assigned to three ranks.

- High weight (Rank is 3): if the function is related directly to the main function, the variability of this aspect affects the main function or goal directly. In Fig. 3, aspects located at level i will have a high weight, so the rank is 3
- Moderate weight (Rank is 2): if the function is not related directly to the main function, but instead to an auxiliary function, the variability of this aspect will affect the main output function or goal moderately or little. In Fig. 3, aspects located at level i-1 will have a moderate weight, so the rank is 2
- Low weight (Rank is 1): if the function is not related directly to the main or auxiliary function, related to a safety function with enough redundant safety functions. So, the variability of this aspect will affect the main output function or goal minimally. In Fig. 3, aspects located at level i-2 will have a low weight, so the rank is 1.

The variability score is determined based on the present performance of functions and aspects and their ideal state. Present performance can be determined by monitoring performance indicators at the previous state. If each aspect is in its ideal situation, variability will be zero. The critical point is to determine the ideal situation. The ideal situation can be assumed as industry best practice. The output will be precise in quality and time if variability is zero. A zero to four variability score table can be created to find the overall output score. Four is the maximum variability state. A maximum variability of 4 means no output from the output function, resources are absent entirely, pre-conditions are not met, or controls are not present.

The following equation is utilized to determine the safety performance of the system:

$$SC_{p,i} = \sum_{j=1}^{m} \left(\left(W_{i,j} * \Delta V_{i,j}\right) + \left(W_{R,j} * \Delta V_{R,j}\right) + \left(W_{PC,j} * \Delta V_{PC,j}\right) + \left(W_{C,j} * \Delta V_{C,j}\right) \right) \quad (1)$$

$$\Delta V_i = \sum_{df=1}^{n} \left((w_o * \Delta v_o) + (w_R * \Delta v_R) + (w_{PC} * \Delta v_{PC}) + (w_C * \Delta v_C) \right) \quad (2)$$

In Eq. (1), $SC_{p,i}$ represents the prediction of the variability of a specific function at a specific time at level i, $W_{i,j}$ Represents the weight of input of jth function of level i. $\Delta V_{i,j}$ represent variability score of input of jth function at time t, $W_{R,j}$ represents the weight of resources of j^{th} function, $\Delta V_{R,j}$ represent variability score of resources of jth function at time t, $W_{PC,j}$ represents the weight of pre-condition of jth function, $\Delta V_{PC,j}$ represent variability score of pre-condition jth function at time t, $W_{C,j}$ represents the weight of control of jth function, $\Delta V_{C,j}$ represents the weight of control of jth function at time t, m is the total number of related safety functions.

In Eq. (2), ΔV_i depends on output function, resources, pre-condition, and controls of its related downstream function df_1 at level i-1. w_o is the weight of the output function of downstream function df_1. Δv_o is variability in precision or time of that output function df_1. w_R is the weight of resource of function df_1. Δv_R is variability in the performance of resources. w_{PC} is the weight of the pre-condition of function df_1.Δv_{PC} is variability in the performance of the pre-condition. w_C is the weight of control of function df_1. Δv_C is the variability of performance of control of function df_1. N is the total number of downstream functions. Similarly, variable downstream functions related to resources, pre-condition, and controls are determined using equation (ii).

3. Case study

STS transfer of LNG is carried out in port. After arrival and mooring of an LNG cargo ship, required tasks include inserting the LNG transfer line, checking storage tank systems and related equipment, earthing, connecting hoses & links, opening the manual and automatic valves, and, finally, starting the pump. After completing the liquid transfer, operators stop the pump, purge the lines, and disconnect the hoses. It is essential to follow the sequence to ensure the safe and proper execution of the transfer. The main component of the STS transfer process is the pump. Other vital components include control valves, motors, hoses, and pipelines. During operation, flexible pipes from the storage tank of the carrier ship are connected to the storage tanks of the storage ship by manifold. Valves are used to control or regulate liquid flow, and thermal relief valves are installed with pipes to control the temperature or pressure of the fluid. The electrical system provides energy to operate the motor driving the pump. An adequate amount of power must be available for the actuators to perform the commands. Modern process systems are equipped with logic controllers or programmable controllers, by which all the components, like pumps and valves, can be controlled. Control room operators can observe all plant operations to ensure everything works correctly. Fig. 4 presents a simplified process flow diagram. Both ship authorities can monitor the transfer conditions, e.g., system pressure, tank volume, and equipment behavior.

3.1. Identify system functions and aspects related to the main goal

The first task is to identify the system goal for which the system is operated. For the present system, the main goal is the transfer of LNG from the carrier ship to the receiver storage tank precisely and on time, maintaining all safety protocols. The main important function related to the goal is the delivery of LNG. There are several other upstream and downstream functions related to this main function. Downstream functions are opening the valve, connecting hoses, and earthing, checking the storage tank, and the arrival of the storage tank. Upstream functions related to the execution of the main function are to stop the pump, purge the line, and disconnect the hose. Aspects pertaining to main functions are also identified. For LNG transfer execution, the output function is delivery complete. The input function is the start of LNG supply at the inlet pipe. Pre-conditions are pre-operational tasks

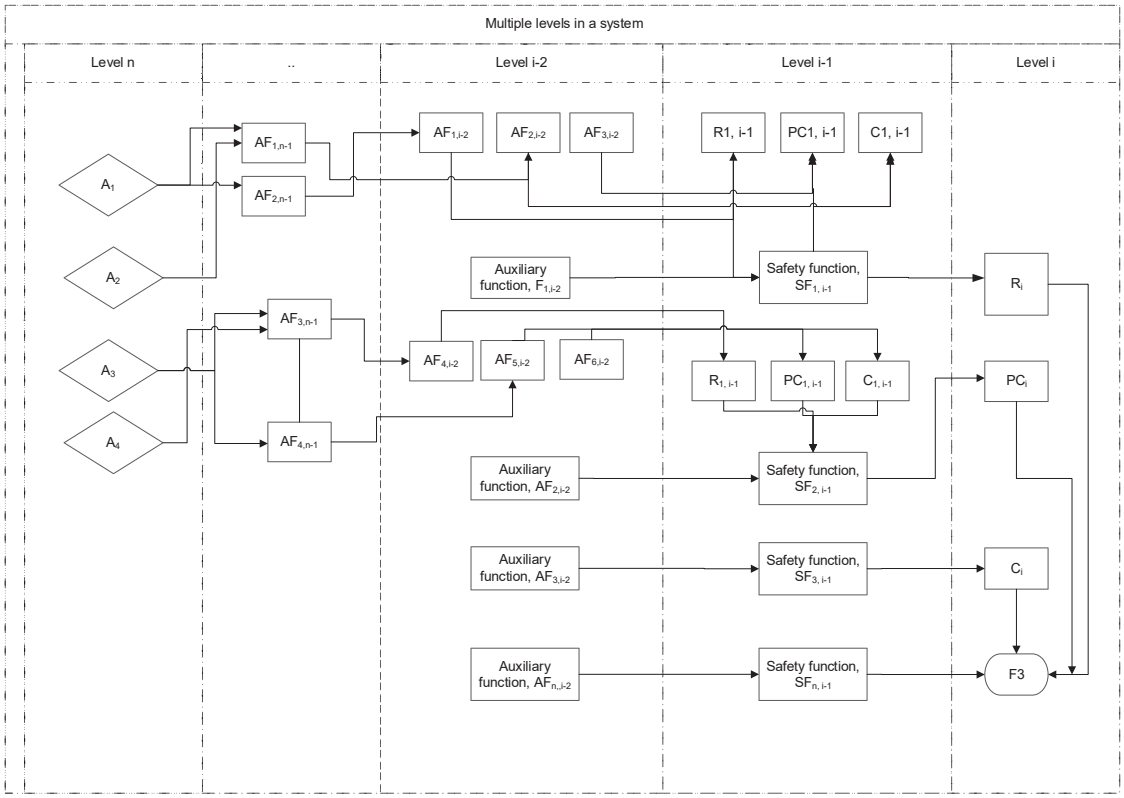


Fig. 3. Contribution of function from multiple levels to the end target function, F3.

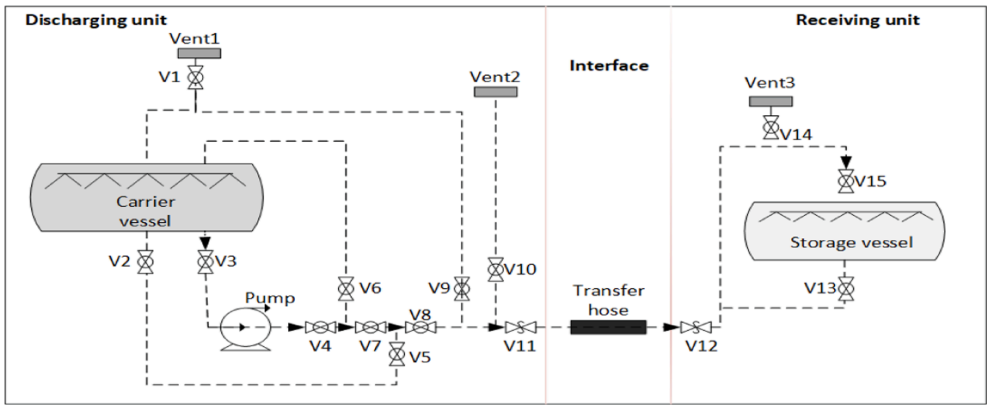


Fig. 4. Process sketch of LNG ship-to-ship transfer procedure.

completed: purging, opening valves, connecting hoses, and checking storage tanks. Resources are all related to equipment, instruments, utility, and procedures. Related equipment is the storage tank, pipe network, pump, and cooling system (Fig. 4). Instruments are thermal relief valves, flow control valves, vent valves, high-level alarms, telecommunications systems, and programmable logic controllers (PLC). Utilities are electricity telecommunications systems. Controls are local operators, PLC, supervisors, plant management, and port authority.

3.2. Determine interactions between functions

Interconnections are shown in the diagram (Fig. 5). If all the aspects are present, e.g., all resources are present, pre-conditions are precise, and controls are functioning precisely, it is expected that functions will be executed precisely and on time, so the goal will be achieved. If any aspect or element of an aspect is missing, it will affect the output function.

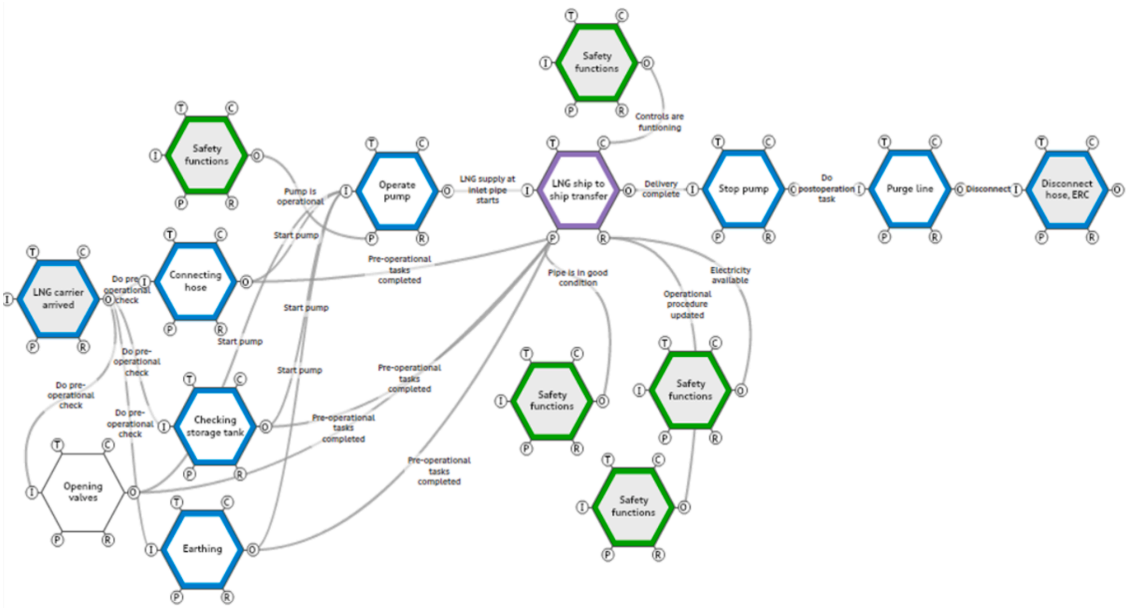


Fig. 5. Steps in LNG ship-to-ship delivery.

3.3. Identify variability in functions and aspects

For LNG ship-to-ship transfer, variabilities are first identified for the main function. For the main function of LNG ship-to-ship transfer, three types of variabilities are: LNG is not delivered at all, LNG could not be delivered in a storage tank in expected quality, and LNG delivery took longer than the target. Variability of aspects of the functions is also identified. The variability of the input function is that pump could not be started. Pre-conditions are varied because pre-operational tasks were not completed, e.g., checking LNG storage tanks, earthing, proper connection of hoses, or opening valves. Variability in resources can be that electricity is not available. Other variabilities in controls can be that valves are blocked or do not work, problems in telecommunication systems, and PLC is not working correctly. Variabilities in control can be the absence of a local operator or plant supervision.

3.4. Identity resonance and causal factors of variability

The causal factors for each variability are identified. For imprecise or deficient LNG delivery, causal factors or variability downstream can be LNG phase changed during transfer or bad LNG quality from the ship. For storage tanks, high-level downstream variability can be related to control and resources. Upstream variability can be a fluid loss. Causal factors evaluated from downstream functions or aspects are identified for each function and aspect. In the same way, the resonance effect in the upstream functions is also specified.

3.5. Identify required safety functions to prevent variability and mitigate variability

Safety functions are identified to prevent variability of the main function. Related aspects of these safety functions are also identified. For variability, LNG is bad quality; a safety function is to adopt a quality check procedure. The input function of this function is to assign personnel for the quality check procedure. Resources can be local operators and quality check procedures. Controls of these functions are plant supervisors. As said earlier, for precise LNG ship-to-ship transfer, all resources and controls should be made available, and pre-conditions should be met before the occurrence of the function. One resource is pipe networks. These are safety barriers as defined traditionally. Several safety functions can be executed to ensure the target function 'keep the pipe network in good condition. If one of the required safety functions is not implemented, still pipe network can work or can deliver its intended function. However, if all safety functions are missing, the pipe network will likely not serve precisely. Various essential safety functions can be pipe check before the operation, regular inspection and maintenance, condition monitoring after a specified period, and pipe insulation to keep the pipe network in good condition. Some downstream functions should be executed to execute these safety functions, e.g., assigning personnel for pipe check, inspection, and maintenance, developing a procedure for inspection and maintenance, and following existing standards. All possible downstream functions should be determined to go into the root cause of a function or aspect variability and keep adequate safety barriers in the system. There can be another scenario also. A pipe network may become deficient for inappropriate downstream safety functions or other external effects. The facility should take action to resist both downstream and upstream resonances.

First, the variability of a function or aspect of a function is defined to find the mitigation barriers of a potential mishap. Then a target function is defined to mitigate the variability. Here, the focus is on mitigative rather than preventive safety functions. A Variability of the pipe network is pipe defect. The related target function is 'to bring pipe network in good condition. Related auxiliary functions are 'to repair', 'mitigate defect', and 'to mitigate further risk'. Related required preventive safety functions are identified and presented in Fig. 6. Mitigative safety functions related to 'bring pipe in good condition 'are identified and presented in Fig. 7.

3.6. Development of safety performance indicators

The result of FRAM analysis, obtained from step 5 of the method (Section 3.5), is utilized to determine the system's performance indicator. The required safety function 'keep pipe network in good condition' (Fig. 6) is translated into measurable quantities, which vary in

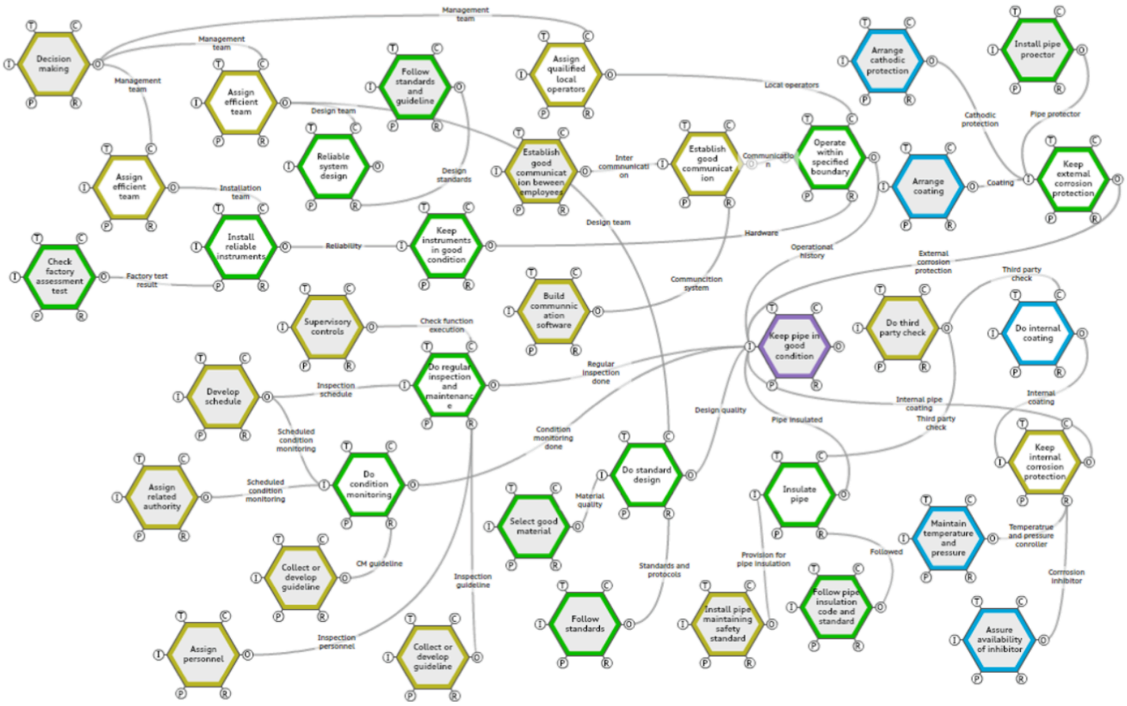


Fig. 6. Required safety functions to keep pipe network in good condition.

duration, frequency, or competency. For the safety function 'keep pipe network in good condition', leading indicators are frequency of condition monitoring of the system, the competence of people for condition monitoring, frequency of maintenance of system, and the competence of people for maintenance. Related performance indicators are developed considering the required downstream functions of 'keep pipe network in good condition. Fifteen indicators are found, which are leading indicators that prevent the event from occurring. Variability functions are used to develop lagging indicators (Table 3).

3.7. Assessment of safety performance of the system

A two-level mathematical model is constructed to determine the safety performance of the LNG STS system; in the present case, two levels will be enough to understand the required functional performance and variability. The safety assessment model is constructed for only a part of the system. The mathematical model includes two required safety functions, ' condition monitoring of pipe network' and 'regular inspection and maintenance due to the limitation of the scope of the present paper. Function execution of pipe checks before operation depends on efficient personnel allocation, procedure development, a balanced workload, and a good work environment. Various subfunctions related to the safety function are given different importance scores considering their importance for executing the function. The final part of the mathematical model is to revise the variability score considering the inter-dependency of the functions and related aspects. The overall score is determined after the revision of the scores (Table 4).

4. Discussion

An extended FRAM method is applied in the paper to check the adequacy of safety barriers and safety assessment of the system. LNG STS system is chosen for the case study. In FRAM, the system is decomposed into system functions. Each function considers input, output, time, control, pre-condition, and resources. Functional relationships can represent human, hardware, and organizational behavior and their relationship. Variability in function is described as output timing and precision. The model shows each element's contribution to a function's outcome. Each aspect has a different perspective and contribution to the execution of a function. While using FRAM for barrier identification gives an idea of how to increase safety measures for executing a function and other relevant requirements.

The analysis in the case study shows how an accident can develop from complex interactions of various imprecise performances. The significant insight from the research is that one minor issue can often significantly impact the system's performance in actual cases. If that minor issue can adequately be handled (Weick and Sutcliffe, 2001), avoiding accidents will increase. In the traditional risk analysis model, often, these issues are neglected due to low probability. Research indicates that even a low probability event can significantly impact the system. The probability and severity of unwanted events will be considerably higher if several significant issues merge into a socio-technical system.

Variability of a function resonances with the variability of other functions or propagates among functions so that the system can deviate much from the acceptable limit. Every entity, including humans, machines, and organizations, plays a vital role in a socio-technical system. The function of each entity, even a single sensor, carries importance from a safety and economic perspective. Each controller's required time constraint, resource availability, and pre-condition fulfillment can be visualized from dynamic analysis. From the gained observation company can act in all possible ways. Confusion arises in assigning duties at the right time and to the proper authority. Function-wise analysis like FRAM can consider both time constraints and authority allocations. It considers both control and time requirements for each function. Redundant barriers are always emphasized in a highly hazardous

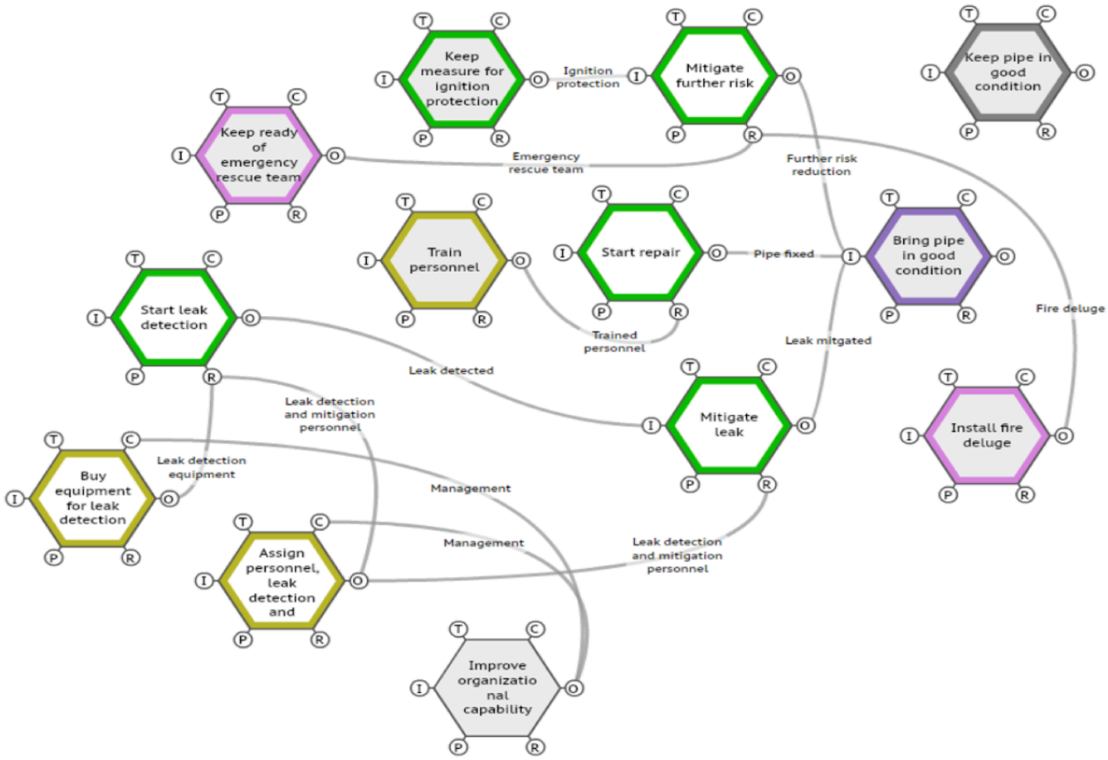


Fig. 7. Required safety functions to mitigate the variability of pipe defect or 'bring pipe network in functional state'.

industry. So even if one barrier fails, the system can still sustain, and production can continue. FRAM analysis can be helpful in consideration of redundant barriers. Variability and resonance can be considered by considering the absence of the required safety function, and alternatives can be sought to execute the main functions and achieve the final goal.

If small missing functions can be identified and mitigative actions can be executed properly, the system's safety can be assumed. Performing each procedure, including supply chain, maintenance within a specified time, and maintaining product quality, carries enormous importance. The benefit of using FRAM is that time constraints for each function execution can be considered individually, and the resonance of missing time targets can also be predicted (Patriarca and Bergström, 2017). Industry can benefit from using such a model to know the required time constraints for individual functions and set pre-required functions accordingly. Also, barrier management or execution of safety functions can be planned therefore based on the weight of the function and their resonance effect of variability in the system.

It is possible to capture variability qualitatively, quantitatively, and dynamically by extended FRAM. The qualitative characteristics of variability can be observed in the visual model of FRAM both for functional output and for outcomes of the entire system. It allows one to capture and visualize functional output variation and understand the nature of functional output variables. Capturing qualitative variability characteristics can help analysts identify sources of variability that influence the output of downstream functions and the entire system. Coupled functions carry great importance as the variability can affect the output of upstream functions and affect related system goals capturing resonance of variability of function.

A prediction variability of a system goal can be expressed numerically by a safety index on a scale of 0 to 4. The numerical number represents a comparative number. However, from the analysis, it is visible that qualitative analysis helps the analysts most by giving critical insight into systems and required barriers. Apart from the variability of performance of related aspects, there can be many uncertainties in the system, affecting the system's performance. Quantitative analysis can compare the system performance at two different times or compare two similar systems. If the calculated safety index indicates the bad performance of the system, actions should be taken to improve the system.

Variability might occur as time variation can affect a function's output or the system's outcome. The model can capture time variation for a specific function and system. The execution time of the function is variable for various cases. The time variability may affect downstream functions in the transition process and may even influence the outcome of the entire system. Understanding time variations can help to improve the quality of the system.

A comparative analysis is done in the paper among extended FRAM, FRAM-STPA, Bayesian network, and bow-tie (Fig. 8). Methods are compared in terms of barrier allocation procedures, risk assessment procedures, competence in hazard identification, competence in barrier allocations, complexity, competence in identifying safety performance indicators, ability to represent complex relationships, acquaintance, and resource and time requirements. While comparing, extended FRAM is considered as described in this paper's method and case study section. The execution method of the FRAM-STPA method is described here, and a case study is presented in the supporting documents of the paper. A traditional Bayesian network and a traditional bow-tie method are considered for the comparison.

The detailed procedure of the FRAM method is described in Section 2 and is explained with a case study in Section 3 of the present paper. In the FRAM-STPA method, STPA keywords are used in the FRAM method

Table 3
Determining performance indicators from aspects of safety functions of FRAM.

Preventive Safety functions	Related aspects	Description	No	Performance indicator
Condition monitoring of pipe (CM)	Input functions	Assign related authority (AA)	1	Competence of authority
		Plan and follow a schedule (FS)	2	Frequency of CM
	Control	Management team	3	Competence of management team
		Maintenance team	4	Competence of maintenance team
		Supervisory control	5	Frequency of supervisory control
		Workplace environment	6	Number of periodical meetings between operators and supervisors
	Resources	Procedure	7	Number of existing procedures on condition monitoring, maintenance-inspection, insulation, operation
			8	Level of detail of each procedure
Do regular inspection and maintenance (RM)	Input functions	Develop schedule	9	Frequency of inspection
	Resources	Personnel (Maintain balance workload, communication, training)	10	Number of training for personnel training
			11	Level of detail covered for each training
		Procedure		
	Control	Supervisory control		
Insulate pipe (I)	Resources	Insulation guideline (FG)		
	Control	Third-party check (TC)	12	Level of detail check by the third party
Pipe design with proper specification (PD)	Resources	Employ efficient team (ET)	13	Competence of design team
		Follow standards (FS)	14	Level of detail of existing standards
Follow the correct operational procedure of STS (FOP)	Resources	Follow standards (FS)	15	Competence of operational team
		Employ efficient employees (EE)		
	Related aspects	Maintain balanced workload		
		Maintain a good work environment		
Keep external corrosion protection	Input functions	Give protection cover		
	Control	Inspection of external corrosion		
Keep internal corrosion protection	Resources	Use corrosion inhibitor		
Mitigative Safety functions				
To repair	Input functions	Assign personnel	1	Competence of repair personnel
		Train personnel	2	Training of personnel
	Control	Management team		
		Maintenance team		
	Resources	Procedure	3	Number of existing procedures and manuals on repair and leak detection
			4	Level of detail of each procedure
Mitigate leak	Input functions	Detect leak		
	Control	Emergency rescue team	5	Competence of emergency rescue team
	Resources	Leak detector	6	Frequency of maintenance of sensors
			7	Frequency of replacement of sensors
			8	Calculated reliability of instrumented systems
		Mitigation procedure		
Mitigate further risk	Input functions	Prevent ignition		
	Control	Management team, Port authority		
	Resources	Deluge for cooling, fire detector, fire extinguisher, sprinkler, emergency rescue team		

to find deviations in the system. The first two steps of this method are similar to the FRAM method. Necessary functions related to the goal and related aspects and interconnections are determined similarly to FRAM. In the next step, deviations of functions and associated aspects are determined. Deviated functions and aspects cannot be marked as precise and proper. A function or an aspect may deviate due to deviation of downstream function or other aspects in the own function or other external aspects. Deviation of function or aspects may affect the system goals in various ways; for example, the system goal is not achieved at all or is not achieved precisely and on time.

Deviation of functions and aspects is identified by applying four key terms of STPA: A required function or aspect is 'not delivered at all, is 'delivered, but causes hazard', 'delivered too early or too late, 'stopped too soon or continued too long. Deviation of functions or aspects occurs due to a deficiency in establishing required safety constraints. Safety barriers are placed on establishing proper causal constraints. Upon failure of those barriers, constraints will not be fulfilled. So, the execution of the related function will not be executed. A FRAM-STPA model is constructed in this paper and presented in a supporting document. No distinction is made between system-level safety constraints and low-level safety constraints. The process model helps to identify causal factors and scenarios. After identifying process model scenarios, necessary safeguards are proposed.

A top event is identified in a traditional bow tie method (Mulcahy et al., 2017). Initiating events/threats and consequences for the top event are identified. Preventing barriers prevents the development of top events from threats (Hollnagel, 2016). Mitigating barriers are barriers to mitigate the effect of the top event to reduce consequences (Ruijter and Guldenmund, 2016). Physical, human, or organizational barriers can be distinguished (Sklet, 2006). The top event's risk can be evaluated by evaluating the performance of preventing and mitigating barriers. Intrinsic safety barriers can be identified to reduce the threats to the system.

A directed acyclic graph is constructed in a Bayesian network model where each node corresponds to a unique random variable. Each edge represents conditional dependency with a connected node. Barriers are

Table 4
Calculation of the possibility of achieving a target function without considering the coupling of performance deviation.

Safety function	Input functions	Weight	Var score			control	Weight	Var score			Resources	Weight	Var score			Effect score		
			Precise	at time t2	Not at all			Precise	at time t2	Not at all			Precise	at time t2	Not at all	Precise	at time t2	Not at all
Condition monitoring of pipe network (CM)	Assign related authority (AA)	3	0	1	4	Management team	3	0	1	4						0	3	12
	Plan and follow a schedule (FS)	3	0	1	4	Maintenance team	3	0	1	4						0	3	12
						Supervisory control	3	0	1	4								
						Workplace environment	3	0	1	4								
											Procedure	3	0	1	4			
	Performance score															0	9	60
	Scaled value															0	0,60	4
Do regular inspection and maintenance (RM)	Develop schedule	3	0	1	4	Supervisory control	3	0	1	4	Procedure	3	0	1	4	0	3	12
											Personnel (Maintain balance workload, communication, training)	3	0	1	4	0	0	0
	Performance score															0	12	48
	Scaled value															0	1,25	4

allocated to reduce the effect of the event or consequence node factors. Assessment in the Bayesian network follows two main steps. Building a directed acyclic graph is the first step. In the second step, conditional probability in each node is assessed for risk assessment of the system.

Hazard identification and mitigation are essential steps of any risk assessment method. The case study shows that both FRAM and FRAM-STPA can be used for hazard identification and mitigation. It is seen that both FRAM and FRAM-STPA can give a good overview of the scenario of system mishaps, and resisting barriers or functions can be better planned accordingly. Using probabilistic data to determine the variability score can evaluate the risk of a mishap. The probabilistic data can be collected from industry data for quantitative risk evaluation. In the present paper, probabilistic data for the assessment is avoided due to time constraints and limitations of the work's scope.

Both FRAM and FRAM-STPA can give a quick way to check the adequacy of safety barriers. From the case study, it is easily visible that both FRAM and FRAM-STPA methods suggest an almost similar number of types and barrier elements required for the system. A significant advantage of the bow-tie model is that it is an easy and time-conserving model to identify barriers and assess risk in the system (Paltrinieri et al., 2019). The Bayesian network can also find the required barriers and determine the effect of the critical barrier in the system. A Bayesian network is built for a part of the case study for 'pipe condition, and a comparative analysis is made. The FRAM model considers the system's status from downstream and upstream functions. Couplings of barriers or interaction of multiple barriers can also be considered.

Safety barrier performance indicators are determined by translating safety functions into measurable quantities. While translating, required input functions, resources, or controls are converted into quantifiable attributes used as indicators. FRAM gives a large number of leading indicators. Leading indicators are developed by extracting attributes related to the required safety function, which can perform the required safety function. In the present case, indicators are developed for only the safety functions of the system. The assessment gives 15 indicators, which indicates that many leading indicators will be found for the entire system. Development of lagging and leading indicators are developed separately. Lagging indicators are developed using the system's variability of function and aspect. Leading safety performance indicators are developed in the Bayesian network by translating attributes of preventing and mitigative barrier nodes into measurable quantities (Fig. 9). The performance indicator of a node represents the performance of that particular barrier node. If performance improves, it will affect risk influencing factors to reduce the risk. For pipe network failure, performance indicators are developed using a Bayesian network and presented in a supporting document. Lagging performance indicators are developed to find frequency of events of safety barrier failures. For pipe network failure, 12 leading and 12 lagging indicators are found, similar to FRAM.

Risk assessment in the FRAM method follows a multilevel mathematical procedure. The variability and weight of the functions are determined using their performance at a specific time. The multilevel mathematical model uses all the assigned scores to find the overall safety index. The safety index represents the safety performance of the overall system. Experts assess weight value based on their expertise and knowledge during weight assignments. Each expert makes their assessment, and the safety performance of the overall system will be determined based on the assigned values. Subjective scoring is a limitation of presented extended FRAM. Different experts may give different scores due to having different educational and cultural backgrounds, work experiences, and familiarity with the project. If various experts are assigned, weighted average values can be used to score. Any mathematical model for risk assessment is not established in the earlier work of FRAM-STPA. Present papers also exclude the effort due to the limitation of the scope of the paper.

In Bayesian networks, A directed acyclic graph depicts a set of variables and their conditional dependencies (DAG). Bayesian networks are

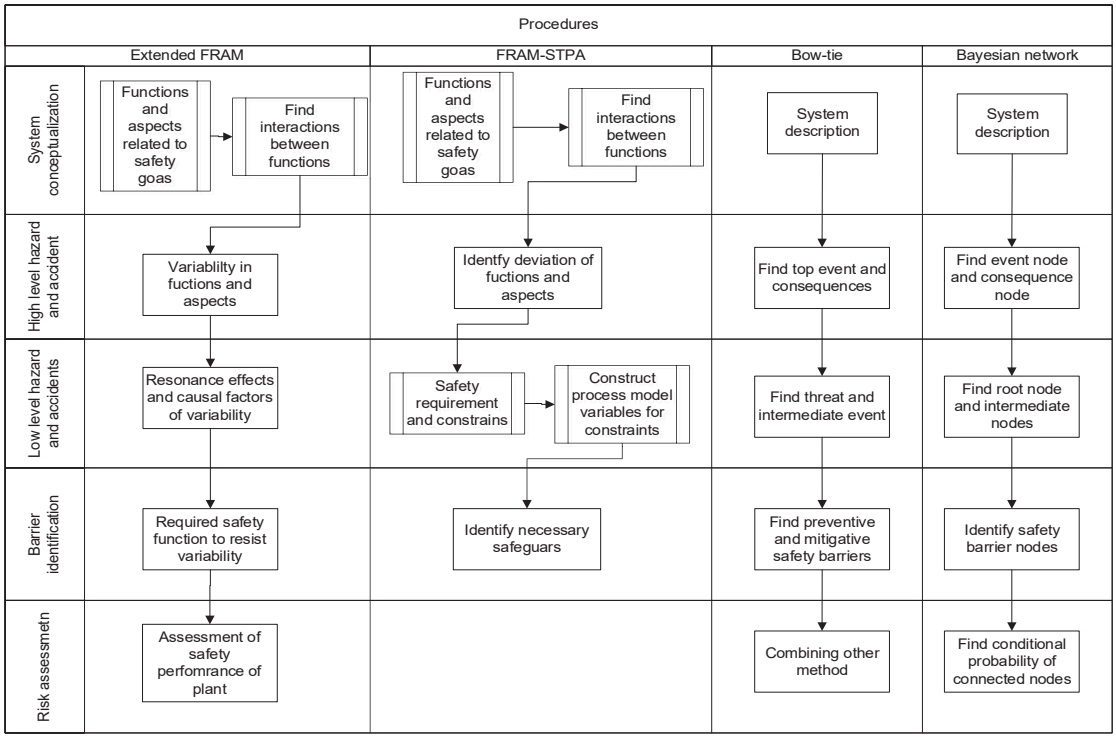


Fig. 8. Procedures of FRAM, FRAM-STPA, Bayesian, Bow-tie.

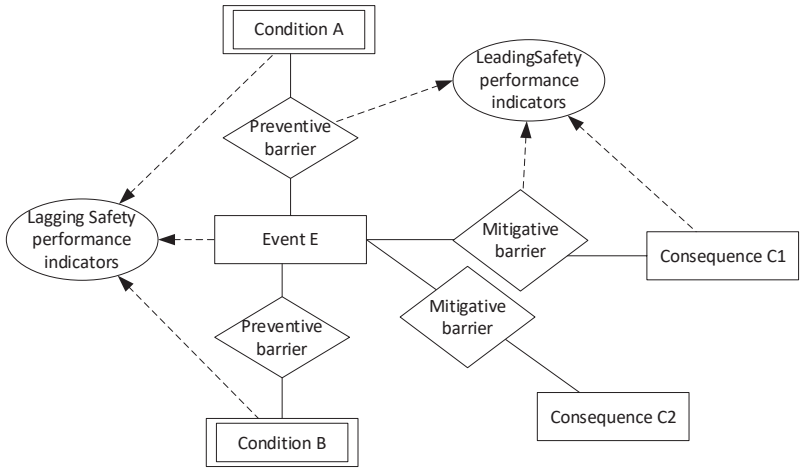


Fig. 9. Barrier allocation and developing safety indicators in the Bayesian network.

suitable for predicting the likelihood of an event knowing the dependence of associated variables affecting the occurrence of an event. Bayesian networks are ideal for forecasting the likelihood of an event knowing the dependency of related variables. A Bayesian network can represent the probabilistic relationships between variables and events. The network can compute the probabilities of the event given causes (Gregoriades and Mouskos, 2013). If an event node exists in the graph connecting random variables A and B, P(E|A, B) is a factor in the joint probability distribution.

In FRAM, resources and controllers are identified for each function execution. So, it can be visible which authority, procedure, or equipment should be assured for function execution. Also, FRAM gives dynamic analysis as it can consider time constraints. The Bow-tie model assumes an accident or mishap created from the contribution of a single threat or a barrier failure (Ferdous et al., 2013). It does not consider any coupling or interaction between threats or multiple barrier failure, which is a

significant limitation in a bow tie. Bayesian network, probability function can be determined to find the relationship (García-Herrero et al., 2013). Change of status with time can also be captured (Yeo et al., 2016). a shortcoming of the Bayesian model is that, in this model, the allocation of tasks or authority of the task is not easily visible.

Compared to Bayesian, FRAM produces more specific details by considering the functional resonance process. Operations can be monitored to understand the entire system's performance once the functional model is constructed. Constructed models provide a basis for identifying potential pathways of both successful and unsuccessful operations. Capturing and interpreting performance variability helps to understand the yay that outcomes of a system (success and failures) are attainted. The study strives to capture variability's qualitative, quantitative, and dynamic characteristics. FRAM model is complex and very new to the industry. Analysts may find it challenging to build the model; hence it will take much time, which is a disadvantage of extended FRAM. Its time-consuming behavior is also proved by the earlier work of.

While determining quantitative performance scores in the extended FRAM method, the scaled value for each safety function is determined where safety functions and their relationship with related functions are relatively simple. For example, condition monitoring of a pipe network is connected to two input functions, four controls, and one resource, where they are linearly correlated. Relationships of other safety functions are considered linear here. Determining performance scores and scaling would be difficult where the relationship between functions and their downstream functions is very complex. The overall performance score is determined for only one required pre-condition to achieve the final goal. Determining the overall performance score for achieving the final goal considering all related input functions, pre-conditions, and resources, will be complicated and cumbersome and require many man-hours. Due to scope and time limitations, complete system analysis is kept out of the scope of the present paper. How to overcome this issue and develop computational tools can be further studied in the future. Involvement of other entities such as government authority, carrier authority, and regulatory authority in executing of function, how reluctance of action of such entities can affect the system's function and may initiate unwanted events are also kept out of the scope of the analysis.

In the FRAM-STPA method, violation of the safety constraints can be translated into risk influencing factors. The maintenance and organizational plans can be improved by considering related risk influencing factors. The bow-tie diagram is used widely in the industry to find the required safety barriers in the system. Bayesian network is also commonly used in industry and academia to show the connection between the system and risk influencing factors. However, considering multiple factors and complex interaction between factors considering each barrier's essential resources or controls gives quite a complex structure. This type of complex structure will take more resources and work hours.

5. Conclusion

This paper presented FRAM analysis for safety barrier management and system risk evaluation. The approach is applied for LNG ship-to-ship transfer operations. In addition, a comparison among bow-tie, FRAM-STPA and Bayesian networks are shown, along with the main conceptual differences between them. Comparison among various methods is based on their barrier allocation procedure, risk assessment procedure, competence in hazard identification, competence in barrier allocation, complexity, required time, and resources. FRAM shows the contribution of each element to the outcome of a function. It gives an idea of how to increase control measures of executing functions and other relevant requirements. The system's status is determined considered from downstream and upstream functions and their status.

The most dominant point in FRAM is that the method can consider the interaction between elements with time constraints, making it suitable for dynamic barrier management. Variability with more detail of the system is possible to extract from FRAM. FRAM possesses a better detail level than the Bayesian network and bow-tie. The paper identifies which functions have a more significant resonance effect in the system. The analysis presented in this article gives insight into how small imprecise or missing functions in the system may lead to substantial mishaps or performance deterioration. Extended FRAM in the presented work includes a semi-quantitative approach to enhance its capability to predict the system's performance.

Bayesian network and bow-tie model has been widely used in industry and academia to show the connection between hazard, consequence, and risk influencing factors. In a Bayesian network, a probability function can find the relationship. The Bayesian model can also consider the coupling of barriers or the interaction of multiple barriers. Change of status with time can also be captured. However, a shortcoming of the Bayesian model is that, in this model, the allocation of tasks or authority is not easily visible. Considering multiple factors and complex interaction between factors considering each barrier's required resources or controls gives quite a complex structure. A disadvantage of FRAM is that it is time-consuming, and presented mathematical analysis is complex. In future work, studying a complex socio-technical system, this type of analysis will help the analysts take the necessary steps to ensure safety and reduce system performance deviation. For example, installing an LNG network in a residential area where a slight deviation can significantly impact the company's reputation and economy.

There can be many types of variability in other systems, such as geographical territory, financial organization, and public administration. These types of systems will require distinct types of measures to prevent system degradation. Degradation relevant to these systems can be identified, and FRAM can be utilized to check measures to avoid such degradation. The consequence of the absence of any measures can also be predicted. Such analysis can be studied in the future. Accidents often occur due to a lack of training and resources in these socio-technical systems. It is possible to find out these lacking by finding required resources or pre-conditions relevant to each function. Many institutions get involved in large-scale projects such as flood prevention, war recovery, and nuclear safety. Often accidents occur from a lack of action from government bodies and related institutions. FRAM can cover the role of various entities. Required actions that the government or related authority should take can be identified, and the consequence of missing action can be predicted. However, a more sophisticated model should be developed to find missing actions from each organization. Future work is needed to understand better and predict these issues. A comparison of various methods in the present paper is made based on the assessment of the LNG STS system, which is quite simple. A complex system may provide various other perspectives on the comparison.

CRediT authorship contribution statement

Sharmin Sultana: Conceptualization, Methodology, Software, Writing – original draft. **Stein Haugen:** Writing – review & editing, Supervision.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Sharmin Sultana reports financial support was provided by Research Council of Norway. Sharmin Sultana reports financial support, administrative support, and article publishing charges were provided by DynSoL AS. Sharmin Sultana reports a relationship with DynSoL AS that includes: employment.

Data availability

No data was used for the research described in the article.

Acknowledgment

The authors like to thank the Norwegian Research Council, Department of Marine Technology, NTNU, Norway, and DynSoL AS for their financial support under research project 283861. The advisory support from team members of DynSoL AS during the research work is also acknowledged.

Appendix A. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ssci.2022.105930.

References

Albery, S., Borys, D., Tepe, S., 2016. Advantages for risk assessment: Evaluating learnings from question sets inspired by the FRAM and the risk matrix in a manufacturing environment. Saf. Sci. 89, 180–189.
Anezíris, O., Gerbec, M., Koromila, I., Nivolianitou, Z., Pilo, F., Salzano, E., 2021. Safety guidelines and a training framework for LNG storage and bunkering at ports. Saf. Sci. 138, 105212.
Anvarifar, F., Voorendt, M.Z., Zevenbergen, C., Thissen, W., 2017. An application of the Functional Resonance Analysis Method (FRAM) to risk analysis of multifunctional flood defences in the Netherlands. Reliab. Eng. Syst. Saf. 158, 130–141.
Aust, J., Pons, D., 2020. A Systematic Methodology for Developing Bowtie in Risk Assessment: Application to Borescope Inspection. Aerospace 7 (7), 86. https://doi.org/10.3390/aerospace7070086.
Belmonte, F., Schön, W., Heurley, L., Capel, R., 2011. Interdisciplinary safety analysis of complex socio-technological systems based on the functional resonance accident model: An application to railway traffic supervision. Reliab. Eng. Syst. Saf. 96, 237–249.
Bensaci, C., Zennir, Y., Pomorski, D., Innal, F., Liu, Y., Tolba, C., 2020. STPA and Bowtie risk analysis study for centralized and hierarchical control architectures comparison. Alexandria Eng. J. 59, 3799–3816.
Davatgar, B.H., Haugen, S., Khakzad, N., Paltrinieri, N., 2020. Integrating FRAM with Dynamic Graph Approach for Risk Analysis during Maintenance Operation. In: Paper presented at the e-proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference (ESREL2020 PSAM15).
De Carvalho, P.V.R., 2011. The use of Functional Resonance Analysis Method (FRAM) in a mid-air collision to understand some characteristics of the air traffic management system resilience. Reliab. Eng. Syst. Saf. 96, 1482–1498.
De Linhares, T.Q., 2021. The combined and phased application of FRAM, STPA, and RAG for nuclear safety management. Universidade Federal do Rio de Janeiro.
Dianous, V. de, Fievez, C., 2006. ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. J. Hazard. Mater. 130, 220–233.
Erik, H., 2017. FRAM: the functional resonance analysis method: modelling complex socio-technical systems. CRC Press.
Fan, H., Enshaei, H., Jayasinghe, S.G., 2022. Dynamic quantitative risk assessment of LNG bunkering SIMOPs based on Bayesian network. J. Ocean Eng. Sci. https://doi.org/10.1016/j.joes.2022.03.004.
Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., Veitch, B., 2013. Analyzing system safety and risks under uncertainty using a bow-tie diagram: An innovative approach. Process Saf. Environ. Prot. 91, 1–18.
Gad, N.A., Abdel-Monem, M., El-Dash, K., Abdel-Hamid, M., 2022. Modeling financial risk contributes to construction projects; case study of expansion food industries. HBRC J. 18, 85–106.
García-Herrero, S., Mariscal, M., Gutiérrez, J.M., Toca-Otero, A., 2013. Bayesian network analysis of safety culture and organizational culture in a nuclear power plant. Saf. Sci. 53, 82–95.
Gregoriades, A., Mouskos, K.C., 2013. Black spots identification through a Bayesian Networks quantification of accident risk index. Transport. Res. Part C: Emerg. Technol. 28, 28–43.
De Andrade Melani, A.H., Silva, D.W.R., Souza, G.F.M., 2014. Use of Bayesian network to support risk-based analysis of LNG carrier loading operation. In: Proceedings of the Probabilistic Safety Assessment and Management (PSAM 14).
Herrera, I.A., Hollnagel, E., Håbrekke, S., 2010. Proposing safety performance indicators for helicopter offshore on the Norwegian Continental Shelf. In: PSAM 10th Conference on Probabilistic Safety Assessment and Management, 2010. 10.
Herrera, I.A., Woltjer, R., 2010. Comparing a multi-linear (STEP) and systemic (FRAM) method for accident analysis. Reliab. Eng. Syst. Saf. 95, 1269–1275.
Hollnagel, E., Goteman, O., 2004. The functional resonance accident model. Proceedings of cognitive system engineering in process plant, 2004, 155-161.
Hollnagel, E., 2016. Barriers and accident prevention. Routledge.
Hosseinniaa, B., Haskinsa, C., Reniersb, G., Paltrinieria, N., 2019. A guideline for the dynamic barrier management framework based on system thinking. Chem. Eng. 77.
Huang, W., Shuai, B., Zuo, B., Xu, Y., Antwi, E., 2019. A systematic railway dangerous goods transportation system risk analysis approach: The 24 model. J. Loss Prev. Process Ind. 61, 94–103.
Johansen, I.L., Rausand, M., 2015. Barrier management in the offshore oil and gas industry. J. Loss Prev. Process Ind. 34, 49–55.
Khakzad, Nima, Khan, Faisal, Amyotte, Paul, 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Saf. Environ. Protect. 91 (1–2), 46. https://doi.org/10.1016/j.psep.2012.01.005, 09575820.
Lee, J., Chung, H., 2018. A new methodology for accident analysis with human and system interaction based on FRAM: Case studies in maritime domain. Saf. Sci. 109, 57–66.
Lee, J., Yoon, W.C., Chung, H., 2020. Formal or informal human collaboration approach to maritime safety using FRAM. Cogn. Technol. Work 22, 861–875.
Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.
Leveson, N., 2011. Engineering a safer world: Systems thinking applied to safety. MIT press.
Li, W., He, M., Sun, Y., Cao, Q., 2019. A proactive operational risk identification and analysis framework based on the integration of ACAT and FRAM. Reliab. Eng. Syst. Saf. 186, 101–109.
Mulcahy, M.B., Boylan, C., Sigmann, S., Stuart, R., 2017. Using bowtie methodology to support laboratory hazard identification, risk management, and incident analysis. J. Chem. Health Saf. 24, 14–20.
Paltrinieri, N., Hauge, S., Nelson, W., 2015. Dynamic barrier management: A case of sand erosion integrity. In: Podofillini, L., Sudret, B., Stojadinovic, B., Zio, E., Kröger, W. (Eds.), Safety and Reliability of Complex Engineered Systems: ESREL 2015. CRC Press, pp. 523–531. https://doi.org/10.1201/b19094-72.
Paltrinieri, N., Comfort, L., Reniers, G., 2019. Learning about risk: Machine learning for risk assessment. Saf. Sci. 118, 475–486.
Patriarca, R., Bergström, J., 2017. Modelling complexity in everyday operations: functional resonance in maritime mooring at quay. Cogn. Technol. Work 19, 711–729.
Patriarca, R., di Gravio, G., Costantino, F., 2017. A Monte Carlo evolution of the Functional Resonance Analysis Method (FRAM) to assess performance variability in complex systems. Saf. Sci. 91, 49–60.
Patriarca, R., Falegnami, A., Costantino, F., Bilotta, F., 2018. Resilience engineering for socio-technical risk analysis: application in neuro-surgery. Reliab. Eng. Syst. Saf. 180, 321–335.
Patriarca, R., di Gravio, G., Woltjer, R., Costantino, F., Praetorius, G., Ferreira, P., Hollnagel, E., 2020. Framing the FRAM: A literature review on the functional resonance analysis method. Saf. Sci. 129, 104827.
Pezeshki, S.I., 2020. Functional Resonance Analysis Method (FRAM) Approach for Barrier Management in Offshore Drilling. Master's thesis, NTNU.
PSA, 2013. Principles for barrier management in the petroleum industry. Petroleum Safety Authority Norway. http://www.psa.no/.
Qiao, W., Li, X., Liu, Q., 2019. Systemic approaches to incident analysis in coal mines: Comparison of the STAMP, FRAM and "2–4" models. Resour. Policy 63, 101453.
Qiao, W., Ma, X., Liu, Y., Deng, W., 2022. Resilience evaluation of maritime liquid cargo emergency response by integrating FRAM and a BN: A case study of a propylene leakage emergency scenario. Ocean Eng. 247, 110584. https://doi.org/10.1016/j.oceaneng.2022.110584.
Rasmussen, J., Suedung, I., 2000. Proactive risk management in a dynamic society, Swedish Rescue Services Agency.
Ruijter, A. de, Guldenmund, F., 2016. The bowtie method: A review. Saf. Sci. 88, 211–218.
Rutkowska, P., Krzyżanowski, M., 2018. FRAM modelling of the transfer of control over aircraft. SJSUT.ST 101, 159–166.
Salihoglu, E., Beşikçi, E.B., 2021. The use of Functional Resonance Analysis Method (FRAM) in a maritime accident: A case study of Prestige. Ocean Eng. 219, 108223.
Sawaragi., T., 2020. Design of resilient socio-technical systems by human-system co-creation. Artificial Life Robot. 25, 219–232.
Seo, D.-H., Choi, Y.-R., Han, O.-S., 2021. Analysis of a Fire Accident during a Batch Reactor Cleaning with AcciMap, STAMP and FRAM. J. Korean Soc. Saf. 36, 62–70.
Sklet, S., 2006. Safety barriers: Definition, classification, and performance. J. Loss Prev. Process Ind. 19, 494–506.
Thomas IV, J.P., 2013. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis. Massachusetts Institute of Technology.
Tian, W., Caponecchia, C., 2020. Using the functional resonance analysis method (FRAM) in aviation safety: A systematic review. J. Adv. Transport.
Tian, J., Wu, J., Yang, Q., Zhao, T., 2016. FRAMA: a safety assessment approach based on Functional Resonance Analysis Method. Saf. Sci. 85, 41–52.
Toda, Y., Matsubara, Y., Takada, H., 2018. FRAM/STPA: Hazard analysis method for FRAM model. Proceedings of the 2018 FRAM Workshop. Cardiff, Wales, 1-17.
Vieira, L.C., Saurin, T.A., 2018. Environmental disaster analysis: case study using the Functional Resonance Analysis Method. Engenharia Sanitaria e Ambiental 23, 373–383.
Weick, K.E., Sutcliffe, K.M., 2001. Managing the unexpected. Jossey-Bass, San Francisco.
Wu, J., Bai, Y., Zhao, H., Hu, X., Cozzani, V., 2021. A quantitative LNG risk assessment model based on integrated Bayesian-Catastrophe-EPE method. Saf. Sci. 137, 105184.
Yang, Ming, 2020. System safety assessment using safety entropy. J. Loss Prevent. Process Ind. 66, 104174.

Yeo, C., Bhandari, J., Abbassi, R., Garaniya, V., Chai, S., Shomali, B., 2016. Dynamic risk analysis of offloading process in floating liquefied natural gas (FLNG) platform using Bayesian Network. J. Loss Prev. Process Ind. 41, 259–269.

Yue, Z., Bin, S., Wencheng, H., Rui, Z., Yu, L., Minhao, X., 2020. Accident evolution mechanism of railway dangerous goods transportation based on FRAM. China Saf. Sci. J. 30, 171.

Zuijderduijn, C., 2000. Risk management by Shell refinery/chemicals at Pernis, the Netherlands. EU Joint Research Centre Conference on Seveso II Safety Cases, Athens.

Paper VI

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 (Sultana et al., 2019a).

Process Safety and Environmental Protection 128 (2019) 107–120

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

Identifying safety indicators for safety performance measurement using a system engineering approach

Sharmin Sultana[a,*], Bjørn Sørskot Andersen[b], Stein Haugen[a]

[a] Department of Marine Technology, Norwegian University of Science & Technology, NTNU, Norway
[b] Department of Mechanical and Industrial Engineering, Norwegian University of Science & Technology, NTNU, Norway

ARTICLE INFO

Article history:
Received 13 November 2018
Received in revised form 24 May 2019
Accepted 24 May 2019
Available online 28 May 2019

Keywords:
Safety
Risk
Performance
Indicator
STAMP
System

ABSTRACT

The paper presents a method for the development of safety indicators for a process industry application based on a system engineering perspective. Traditional approaches use probabilistic risk assessment or linear accident models which assume that accidents are linear chains of events and do not consider complex systemic factors and interactions. After BP's Texas City refinery incident, the investigation committee reported that BP had a false sense of safety performance due to providing more focus on managing personal safety rather than process safety. System engineering concepts may help the process industry to operate their activities without any severe accidents by establishing a better safety management system. This paper adopts the STAMP (System-Theoretic Accident Model and Processes) accident causation model to identify system specific indicators and also describes the proposed method with the help of a simple process industry application which is an LNG ship to ship transfer process. It compares the developed method with other methods for practical case applications. The first step of the present method is to establish the safety control structure, then safety performance indicators are identified. Further work is necessary to investigate to what degree these STAMP based indicators are complementary to indicators developed by other methods.

1. Introduction

An indicator is a measurable representation of the aspect of reality. Safety indicators provide feedback about systems to ensure that controls systems are in the safe envelope of design. They are usually linked to a target to determine if they are on track concerning goal, objective, and required actions (Bellamy, 2012). The industry can improve the effectiveness of the safety management system by focusing on the most critical issues concerning hazards and risks. Safety indicators can be used to monitor the level of safety in a system to provide the necessary information for decision-makers about where and how to act (Hale, 2009). However, in the process industry, it is not easy to establish a relationship between system discrepancy and process safety. Often the challenge involves developing reliable and constant indicators that can measure safety performance effectively.

Looking back to history, the first two publications on safety indicators was the work of Rockwell (1959) and Tarrants (1963). Rockwell looked for a measure of safety performance on occupational safety following Heinrich's domino metaphor as the starting point. Tarrants also adopted the same approach that accidents always precede by error or unsafe conditions or a combination of error. He proposed to include incidents and accidents as a basis for indicators. In the academy, two different perspectives have mainly led to the development of performance indicators: safety performance indicators and risk-based indicators. They serve the same purpose but originates from different points of view. In risk-based indicator models, the risk model includes all risk influencing factors (RIF), so it is possible to determine the effect on risk for a change in the indicator value of a given RIF (Øien et al., 1997; Vinnem et al., 2003; Haugen et al., 2012, Øien, 2001a,b, Vinnem, 2010).

Safety indicators model do not have such a risk model. The indicators and the corresponding factors are then often selected, based on either an assumed effect on safety or through correlation (Øien et al., 2011), (Basso et al., 2004). They identify possible safety flaws during or before the operation following various ways, e.g., from accident causation model, through incident analysis, historical facts, prior knowledge, simulation, vice versa. Development of safety indicators based on accident causation model adopts various accident models, e.g., Reason's domino metaphor (Reason, 1997), Heinrich' accident pyramid model (Heinrich, 1931), swiss cheese metaphor, vice versa. Accident models try to explain why accidents

* Corresponding author.
E-mail address: sharmin.sultana@ntnu.no (S. Sultana).

https://doi.org/10.1016/j.psep.2019.05.047
0957-5820/

happen, focus on different aspects, and tries to find the cause-effect chain that finally leads to an accident. Indicators are developed based on the holes in the risk control system (UK HSE guideline, 2006). Heinrich's accident pyramid model follows the concept that many precursor incidents occur with lesser consequences before occurring an accident with high (CCPS, 2007).

Researchers (Tarrants, 1980; Guastello, 1993; Mearns et al., 2003; Clarke, 2006; Forest and Kessler, 2013) have tried to establish general relations between safety performance and contributing factors, i.e., the quality of safety management elements or the adequacy of the safety climate. It has been difficult for safety, health, and environmental (SHE) professionals to establish numerical cause and effect relationship related to indicators chosen. Most of the literature does not contain mathematically or scientifically supported evidence that shows a quantitative relationship between the ïndicatorsänd prevention of accidents. The occurrence of an accident does not say anything about the quality of installation, personnel, or management (Ale, 2009). Similarly, even if everything functions as intended, there remains a probability that an accident will occur. Safety management failure may have a blind spot and may only be visible in times of more massive scale accident.

Inadequate correlation between safety indicators with process safety performance and safety management system has resulted in accidents like the Ciniza oil refinery explosion (CSB, 2005), the Mexico City refinery accident (Lees, 2012), the Balongan LPG Plant accident (Clough, 2009) and BP's Texas City refinery accident (Baker et al., 2007). Of these accidents, BP Texas city explosion carries the most vital importance in terms of process safety performance. BP was much reliant on injury rate as a measure of process safety performance at its US refineries before the Texas City Accident and was ignorant about the risk of process-related incidents or overall performance of its process safety management system (Baker et al., 2007). Process safety elements such as mechanical integrity, training, leadership, and Management of Change (MOC) were deficient despite having excellent personal safety performance (Baker et al., 2007). BP's insufficient measure of loss of containment incident and outcome indicators has early warning of disaster but had fallen in management's blind spot (Hopkins, 2008). Similarly, Esso gas plant at Longford was managing its significant hazards quite poorly despite having low lost time injury rate (Hopkins, 2000). The industry could have prevented accidents by implementing proper control actions as it knew many of the problems before the disasters (Benner, 1975; CSB, 2007; Mogford, 2005).

Heinrich triangle-based models follow the use of near-miss data, but the meaning of near-miss data should be more precise to evaluate best such more frequent data including the risks associated with deviations as well as the safety management strengths and weaknesses. Körvers and Sonnemans (2008) raised the question about whether collecting data of these small-scale accidents is enough to establish an effective safety management program.

For a decade, lost time incident frequency (LTIF) had been used as a key safety indicator in the process industry. LTIF represents the number of days of absence to work due to an accident, per million hours worked. According to experts (Hale, 2009; Ale, 2009), LTIF figures cannot be regarded as indicators of process safety. In the case of using this, the plant should find the relationship between LTIF and the probability of accidents. LTIF and probability of accidents may not have the same causes and the same accident mechanisms. This criterion depends on the specific situation, whether LTI is in the causal chain of significant disasters.

Risk indicators are often derived using Quantitative Risk Analysis (QRA) model. QRAs are established on the causal relationship, based on the deficiencies in process safety management and links the outputs to shortcomings in the technical system component through an influence on their probability of failure. A problem of this concept is that the best way to measure socio factor to incorporate these into risk assessment is unknown (Bellamy, 2012). Small scale accidents can be an indicator for a larger one if small accidents are part of the same population of accidents of a larger one (Ale, 2009).

A sizeable missing piece in today's existing approaches is the lack of integration in the control of safety between technical entities and management/organizational entities. A safety management system can be fully capable only when it considers the full system, along with its complex interaction within its subsystems, dynamics, and if communication with its subsystems is proactive enough to enable early action (Rasmussen, 1997). Basso et al., 2004 have worked on reviewing safety management system by incident investigation and performance indicators, which operators often disregard.

This paper adopts a system-based model to address system aspects that allow detection of ineffective control and degradation of the system. It fosters STAMP based modeling (Leveson, 2004) to develop leading indicators. STAMP considers as a system control problem instead of "prevent failure" problem. In Leveson's paper (Leveson, 2015a), the author presents a proactive method of identifying and operationalizing leading indicators as warning signals based on the STAMP model for aviation system. The STAMP model includes traditional component failures but also considers design flaws, incomplete or inadequate requirements, dysfunctional interactions among subsystems or components, human interactions, and other causes of accidents and incidents. With STAMP, the emphasis changes from simply preventing failures from enforcing constraints on system behavior and interactions. One has to define the system boundaries, to identify the hazards to the system, the safety constraints, and to find all control loops, to obtain an integrated view of what can go wrong.

The present paper performs two main tasks. The first task is related to the development of system-based safety indicators. The second task is to make a comparison between the present developed method and another traditional method already used by industry. The first task starts by searching for the causes of accidents of a system and further searching for causal factors, including technical, human, and organizational purposes by establishing a relationship between a system and its controllers.

The paper develops system-based process safety indicators for an LNG floating storage platform. Technical and organizational safety indicators are established to ensure an effective control structure. The control structure then can help plant managers and decision makers in proactive risk management by monitoring contributing factors in systematic ways to prevent accidents before they occur. This paper compares the indicators developed following STAMP to those derived following the guidance of OECD (2003) and CCPS (2010).Ṫhe following section describes an overview of previous work for the development of performance indicators. The M̈ethodologyS̈ection describes the method of the present analysis and the Äpplications̈ection presents the case study before discussing in the D̈iscussions̈ection. The final section, "Conclusion," states the conclusions.

2. Previous research on the development of indicators

This paper performs a literature review mainly in the nuclear industry and the process industry, as the nuclear power industry has been a critical driver in the development of significant hazard indicators.

2.1. Development of indicators in the nuclear industry

Two crucial directions in the industry were real equipment performance safety and operational performance safety. World

Association of Nuclear Operators (WANO) established global standardization of performance indicators after the Chernobyl accident in 1986 (Reason, 1987). In 1990, WANO found a set of ten performance indicators in the areas of nuclear power plant safety, reliability, efficiency, and personal safety (Holmberg et al., 1998). Still, there raised concerns regarding the extent of safety emphasis in the WANO indicator set. A practical problem for the operators is to sort out the most crucial information from the massive information flow that comes in every day. More power plant-specific safety indicators can enhance knowledge. Thus, further development and implementation of more accurate and plant-specific indicators) were considered useful among nuclear plant operators as well as regulators (IAEA, 2000; Holmberg et al., 1998).

The WANO indicators have direct and indirect indicators. Direct outcome indicators utilize different types of experience data with emphasizing the development of indicators that can give early warnings. These early warning types of indicators are classified as indirect indicators, which can measure the performance of the functional units within an organization, such as operation, maintenance, training, and engineering support (Holmberg et al., 1998).

Nordic project (described by Laakso et al. (1994)) used the barriers in the defense-in-depth strategy along with identifying risk analysis as a framework for identification and structuring of the safety performance areas. Barriers are physical or nonphysical systems which prevent energy from getting out of control, thereby reducing risk to assets and human beings. They should uphold the integrity for a defined time and energy limit. The performance areas defined, based on the defense-in-depth strategy, were: Safety management (Level 1 safety barrier), Control of operation (Level 2 safety barrier), Safety functions (Level 3 safety barrier), Physical barriers (Physical barriers 1–4). Indicators can be used to evaluate safety by assessing the performance level, and by determining the performance trend. Vattenfall developed operator specific safety indicators in continuation of the Nordic project. Holmberg et al. (1998) developed and tested risk-based PSA indicators. They used risk follow-up of events and unavailability of safety-related systems as the indicators. The main aim was to classify the safety significance of events, and not to use the indicators as a tool for c̈ontinuousr̈isk control.

The development of the IAEA framework (2000) for indicators began with the consideration of the concept of nuclear power plant safety performance. The frame structured on two levels. The top level was operational safety performance, and the second level was operational safety attributes. Three essential aspects were addressed to define the key characteristics – nuclear power plant regular operation, emergency operation, and the attitude towards personal safety. The frame establishes overall indicators below each attribute. A level of strategic indicators is defined associated with each overall indicator, intended to provide a bridge from overall to specific indicators. Finally, each critical indicator was supported by a set of specific indicators, which represent quantifiable measures of performance (Gómez-Cobo, 2002). In this framework, only the indicators are measurable quantities, and higher-level indicators can measure in physical quantities. Higher-level indicators provide a qualitative assessment.

2.2. Development of indicators in the process industry

Experience from the nuclear industry is not necessarily helpful in the process industry. In the process and chemical industry, the different manufacturing processes, products, technologies, and chemical properties, represent a much broader spectrum to be addressed. The process industry has adopted various accident models for the development of indicators. In the non-nuclear process industry, development of indicators has been viewed mainly from three main accident perspectives, the Energy barrier perspective, the Resilience engineering perspective, Functional resonance analysis method and the System dynamic model perspective.

2.2.1. Energy barrier perspective

Gibson (1961)) introduced the Energy Model, saying that the more natural way to classify the accidents is according to the physical energy form involved. Haddon (1968) did further work for accident prevention. The main idea is that accidents occur when targets are affected by bad energy in the absence of effective barriers between the energy source and the object. Reason (1997) Swiss cheese model uses an energy barrier perspective. Accidents occur due to holes in the barriers and safeguards. In an ideal world, all protective layers should be intact, allowing no penetration to happen. However, in the real world defenses may deteriorate over time (such as the corroded sprinklers on Piper Alpha Paté-Cornell (1993)). Modification or redesign may weaken or eliminate defenses. Defenses can be removed during calibration, maintenance, and testing or as a result of errors and violations.

In 1994, the NPD initiated a pilot project (Nielsen et al., 1996; Øien et al., 1997, 1998) with the purpose to develop a set of indicators to measure changes in risk level during the operation of petroleum platforms. Quantitative risk analysis (QRA) was used to identify risk indicators giving the most significant contribution to the total risk. There was another followed pilot project which developed a set of risk indicators for a specific installation (Øien and Sklet, 1999).

Øien (2001b) developed a risk-based method to cover the total risk picture. The model hypothesized that in control of changes in the risk influencing factors (RIF) included in the risk model in the QRA. The model did not cover n̈on-technicalr̈isk indicators (human and organizational factors). Øien (2001a) developed organizational risk indicators based on an organizational risk influence model (ORIM) resembling previous organizational factor frameworks (Embrey, 1992; Murphy and Paté-Cornell, 1996; Papazoglou et al., 2003; Davoudian et al., 1994a,b).

OECD started in 2003 to give guidance to the process industry at large through the Chemical Accidents Programme. This described method start by identifying critical potential hazards in various areas of concern that are most critical to control risk. Indicators are developed based on potential failures in the areas of concerns, or where there are ineffective barriers. The main new contributions of this guideline were differentiating outcome indicators (lagging) from activities indicators (leading) along with additional details on their development.

Vinnem et al. (2010) describe the risk level project of the Petroleum Safety Authority to identify levels of risk from indicators. Vinnem distinguishes technical barriers from the human element. They developed technical barrier indicators of safety-critical systems with measures of test success/failure reported by the installations for these barriers such as emergency shutdown valves, fire detection, and pressure safety valves. Barrier performance panels can be updated every 3 or 6 months with a rolling 12-month average, showing status and trend direction which would maintain motivation and awareness on the significant hazards. However, barrier performance did not correlate significantly with hydrocarbon leaks (Vinnem et al., 2010).

The risk model developed by RIVM (Dutch Ministry of Social Affairs and Employment) used accident data as a basis for logical modeling (Bellamy, 2012). The model is built by organizing the precursor events from the accident analysis and relating these to results using probabilistic modeling. The logical model, therefore, lacks the sociotechnical element.

Khan et al. (2010) presented a risk-based approach where they used a risk metric to classify process safety. A hierarchical risk aggregation approach was used to aggregate indicators. They developed safety performance indicators (SPI) following UK HSE

guidelines (2006). The risk factor for three integrity categories: operation, mechanical, and personnel are aggregated using the weighted average approach. The industry can monitor the three elements through a set of parameters and sub-parameters characterized by two groups: leading and lagging indicators.

Haugen et al. (2012) developed a method to identify indicators not only related to operations and technical systems directly but also to planning processes and other preconditions. The technique uses a risk influence model to identify factors that influence the probability of a specific event. For each element, indicators can measure the status of the factors. Sharp et al. (2008) developed key performance indicators for offshore structure integrity based on barrier analysis. Performance indicators were designed to monitor those barriers with quantifiable measures. Øien (2008) explores the possibility of developing early warning indicators based on the incident investigation. He analyzed the incidents using influence diagrams, and from them identified seven general barriers against hydrocarbon leaks. Further, he recognized both checkpoints and indicators for each barrier, which provide information about the status of barriers and the early warning of potential spills.

The UK HSE guidance (2006) describes a method based on the Swiss Cheese model. A vital addition of this guidance was the introduction of the dual assurance concept requiring both leading and lagging indicators. Leading indicators are developed based on barrier failures that are discovered during reviews, while lagging indicators are generated based on failures after an incident or near-miss has occurred.

Many scientists (Scarponi et al., 2016; Pasman et al., 2013; Zhang et al., 2016) have used Bayesian network as a risk model and developed performance indicators based on the model. Haugom and Friis-Hansen (2011) used a Bayesian network to model risk in a hydrogen refueling station. Gerbec and Kontić (2017) also used a Bayesian belief network to establish process safety-related performance indicators. Their case study deals with ship tanker unloading of methanol at a liquid cargo terminal. Zhao et al. (2015) also used the Bayesian network modeling to analyze risk on LNG carrier anchoring system.

2.2.2. Resilience engineering perspective

Resilience Engineering is not about assessing accident risks, but also assessing the organization's ability to be resilient (succeed) in the face of expected and unexpected events. Øien et al. (2010) describe a method for the development of early warning indicators based on resilience and resilience engineering (REWI). REWI method originates from a technique developed by the U.S. Electric Power Research Institute (EPRI) known as Leading Indicators of Organizational Health (LIOH) (EPRI, 2001, 2000). REWI consists of three main parts. The first part is a set of contributing success factors being attributes of resilience, the second part is general issues to fulfill the goal of each contributing success factors, and the third part is the indicators established for each general point. Final selection of indicators may include indicators created by other approaches.

According to Paltrinieri et al. (2012), the dual assurance method (HSE, 2006) strictly depends on the results from the HAZID process. A lack or flaw in the HAZID process would affect all the subsequent analyses and will not recognize an accident scenario. On the other hand, REWI is not dependent on the specific HAZID outcome. It is complementary to the result of HAZID and supports risk appraisal through a parallel and comprehensive action of organizational improvement.

Thieme and Utne (2017) used both dual assurance method and resilience-based early warning indicators (REWI) method to develop safety indicators of the autonomous marine system. They showed in their paper that these two methods are complementary. If two methods are applied separately, they overlook essential safety aspects. Whereas, if combined, gives complete coverage of safety aspects. Developing safety indicators is most efficient if implemented during the design stage and can be refined based on operational experience. Implementation during the operational phase is challenging due to various interfaces. For an autonomous vehicle, they developed five outcome and eleven early warning indicators. Developed indicators cover direct safety function, e.g., alarm and broader safety function, e.g., maintenance.

Functional Resonance Analysis model (FRAM) is based on resilience engineering principles and is used to identify leading indicators (Hollnagel, 2017a). FRAM comprises five steps, which are: to identify system functions, to assess and evaluate potential variability of each function, to identify functional resonance using instantiations and to identify effective countermeasure or barriers existing in the system. FRAM modeling provides a dynamic approach which is necessary for dynamic operation e,g, helicopter operation (Herrera et al., 2010). The use of instantiations enables to illustrate how variability spreads and which variability is significant to a successful operation. It considers the influence of the context on actual performance.

2.2.3. System dynamic model

Systems modelers, e.g., Hollnagel and Woods (2006), consider the concept of a chain of causes or holes in slices of cheese too linear. The graphical modeling of fault and event trees is too constraining. The system modeling perspective looks at the hierarchies of control and conceptualizes the whole system as one entity, not as being made up of several components. STAMP (Systems Theoretic Accident Modelling and Processes) model integrates all aspects of risk, including organizational and social (Leveson, 2004). An essential element is a 'constraint'. The modeling makes sense for controlling safety systems with their dynamic boundaries. The control hierarchy has downward communication imposing constraints and has a measuring channel to provide feedback about effective constraint enforcement. The present paper adopts STAMP based model. The following section describes the detailed procedure of the method.

2.3. Difference between leading and lagging indicators

There has been much dispute among safety professionals and researchers about the definition and use of lagging and leading indicators. The first dispute is on the meaning of the terms. Hopkins (2009) defined leading indicators as "precursors of harm" as opposed to lagging indicators that are "direct measures of this harm". Kjellén (2000) defined a safety performance measure or indicator as to the metric used to measure the organization's ability to control the risk of accidents. In practice, this means to measure directly or indirectly, the level of risk of accidents (probability, consequence) and how this develops over time. A leading safety performance indicator is, in this interpretation, a sign that changes before the actual risk level have changed.

The Swiss cheese model describes accidents as a series of failings (holes) in the layers of defenses or barriers. According to this model, leading indicators identify gaps in the risk control system, whereas the lagging indicators reveal the holes in the barriers because of an incident. Hollnagel (2017b) has discussed these issues from the system engineering perspective. According to his theory, leading indicators can be created based on the sense of perturbations in the parts of the system where fluctuations may be observed to see how stable the system is. In contrast, lagging indicators generally provide evidence of an effective safety system by finding any unlikely consequences of changes.

According to Erikson (2009), lagging performance indicators are focusing on the output and are indeed providing the best measure of how well the management system is performing. The leading performance indicators are concentrated on the input and describe how to achieve the primary objective and how to improve it. In

this sense, there is a fundamental difference between leading and lagging indicators, and both are needed to determine how well the organization is managing the process safety. A specific indicator could be lagging concerning one objective while leading concerning another. Failure at testing is lagging concerning the performance of the individual barriers, while leading concerning the performance of the overall process safety management system.

According to Hopkins (2009), lagging indicators are not very useful as pre-warnings or early warnings. For early warnings, one needs to look further back in the causal chain at the underlying causes and the condition of the factors that lead to accidents. These causes or conditions are proactive or leading indirect indicators. Hopkins bases his argument on the fact that the bowtie model does not provide a reasonable basis for the distinction between lead and lag. According to Vinnem et al. (2006), leading indicators are preferable over lagging indicators. There is more motivation in reporting performance of preventive measures, compared to performance in the occurrence of near-misses. If the data collection scheme is limited, the number of faults recorded are insufficient to make a reliable decision. In that case, leading indicators are preferable over lagging indicators.

HSE guideline (2006) emphasizes the importance of utilizing both leading and lagging indicators and use the term 'dual assurance.' According to Grote (2009) and Kjellén (2009), the starting point could be to establish the purpose of indicators, describing the functions that they may have. Several authors do not distinguish between leading and lagging anymore. They (Saqib and Tahir Siddiqi, 2008; Grote, 2009; Mearns, 2009; Øien et al., 2011) use general terminology, like a key indicator, safety performance indicator, or key performance indicators. There is vast literature which worked on the development of leading and lagging indicators in various applications and performed comparative studies between them. In 2012, the European Process Safety Centre (EPSC) published making a case on the selection, development, and implementation of leading indicators for process safety (Knijff et al., 2013).

Lingard et al. (2017) examined the temporal relationships between the safety performance indicators, including traditional lagging indicators, as well as expected leading indicators for a construction process. They uncovered time-dependent relationships and explored causal relationships between indicators. The analysis revealed complex interactions between safety indicators over time. They found that the expected leading indicators behaved as both leading and lagging indicators concerning the project total recordable injury frequency rate. Sheehan et al. (2016) considered the association between leading and lagging indicators of OHS. They investigated the moderating effect of safety leadership on the association between leading and lagging indicators. The association provides information to focus more on leading indicators instead of lagging indicators.

Jablonowski (2012) presented the study of leading safety indicators using regression of a data set from an onshore drilling operation. The analysis suggests that a viable leading indicator exists in the form of a lagged specification on of the oil company's present safety metrics. Additional analysis of the leading indicator suggests a critical threshold for intervention.

Herrera and Hovden (2008) developed leading indicators for maintenance of aviation in the context of resilience. Leading indicators are precursors based on a model of safety, implying a significant possibility of a subsequent event that has an impact on safety and performance. Leading indicators can, therefore, provide information about changes in risk before traditional risk analyses can capture this change. Other notable works include the works of Sinelnikov et al. (2015); Grabowski et al. (2007); Hinze et al. (2013); Robson et al. (2017b); Jablonowski (2012); Guo and Yiu (2015); Robson et al. (2017a); Nelson et al. (2016); Reiman and Pietikäinen (2012); Khawaji (2012).

3. Methodology

According to STAMP, safety is an emergent system property, and accidents are caused by unwanted interaction among system component that violates system safety constraints. An example of a safety constraint is that the plant should store a highly reactive chemical below a maximum temperature. The plant should enforce this restraint in the operating process and should take contingency actions in case of violation of the constraints. STAMP views system safety as a control problem. Accidents occur when the system cannot control its components (physical and social). The controls can be managerial, organizational, physical, operational, or manufacturing. Major accidents occur due to not only component failure or human error, but also from weak enforcement of safety constraints on design, construction, or operation of the entire sociotechnical system (Leveson, 2015b).

The present paper develops safety performance indicators using the STAMP method. Hazard analysis in STAMP method is performed using the STPA method. Execution of the process consists of the following steps:

1 Define the scope of safety indicator development program
2 Description of system boundaries and the control structure of the system
3 Identification of system level hazards, accidents, and safety constraint
4 Identification of required control actions to keep the system safe
5 Identification of the low-level contribution factors or scenarios that results in hazardous situations
6 Determination of corrective actions to rectify the hazardous causes
7 Identification of safety performance indicators
8 Development of a performance monitoring program

3.1. Define the scope of safety indicator development program

The first step is to establish the scope of the safety indicator development program. The aim is to identify essential safety indicators. Scope includes a description of the system, significant hazards, associated safety barrier, and safe operational limit. In the context of LNG ship to ship transfer, the focus of an indicator system could be on the vessel and control center. For this system, significant hazards are a loss of containment.

3.2. Description of system boundaries and control structure

Based on the scope of the indicator development program, the boundary of the system is defined. The next step is to conceptualize the system as a control system. This step is related to the collecting and compiling of information and data about the system, site, and associated activities under analysis. A control structure is created using the system requirements and interactions. Each different entity performing a specific action is identified to build the control structure.

In a system, controllers provide actions to keep the system under control. Feedback entities give information to the controller about the latest state of the system. Feedback may be from a physical entity or by an automatic process. For example, automatic detectors or logic sensor may send information to the controller about the state of the system or a human operator may be informed from physical detectors or sensors and may act. The controller then gives the command to an actuator to take necessary action if required. In modern process systems, controllers are automated logic controllers in most cases or a human operator in specific instances.

The actuator goes to the necessary state or executes the action as per it gets a command from the controller. For example, a pressure

relief valve opens when the controller gives a command to reduce pressure getting feedback from the pressure sensor that pressure is too high in the system. In a specific situation, a human operator may act as an actuator, e.g., a local operator may reduce pressure manually. Other actuation systems can be pumps, motors, speed controller, etc. In STAMP, not only technical systems and humans can only act as controllers. Organizational system elements such as policies, procedures, and organizational culture may also serve as controllers.

The control structure shows the responsibilities of each controller, along with system behavior and existing feedback mechanisms between different responsible entities (controllers) in the system. The system can consist of various controllers, actuator system, and disturbance processes (e.g., wind, waves, current). A Control Structure diagram provides the means to visualize the interactions between the controller, actuator, and actual procedure. It provides an in-depth means for identifying potentially hazardous control actions by identifying system behaviors and interactions. It illustrates the paths for inadequate control of the system that can lead to a dangerous state.

3.3. Identification of system level hazards, accidents, and safety constraints

After the construction of the control structure model and the control hierarchy, the next step is to identify unsafe control actions that can lead to hazards. STPA follows a step by step procedure to identify risky control actions. In STPA, a hazard is a system state or set of conditions that, together with a set of worst-case operational and environmental conditions, lead to an accident (loss event). In process systems, it is beneficial to identify an intermediate accidental event. An intermediate accidental event is an event in a sequence of events that upsets normal operations of the system and if not controlled, may lead to an unwanted accidental incident or accident. An example of an intermediate accidental event is 'leak in the system,' which, if not controlled, may lead to a fire or explosion if ignited. Confusion may arise in the definition of hazard and intermediate accidental event. Hazard is the beginning of a process upset, or a disturbance of the system which if not controlled, may lead to intermediate accidental event or accidents. For example, a hazard is a high temperature or pressure or another undesired situation in the system from which a leak may occur which in turn is an intermediate accidental event. The table (Table A.2 in Appendix) shows a list of hazards and accidents for the present system.

Safety constraints are those criteria that must be enforced on the behavior of the system to ensure safety. If the system cannot control the hazards, they may lead to accidents. Present method searches for necessary control actions which should be executed to keep the system safe. For example, a hazard (high temperature or pressure), if not controlled, may lead to an intermediate accidental event (unexpected leak) or accident (fire or explosion). The necessary control action is to keep the temperature or pressure of the system under a threshold limit. Each controller should perform as expected to maintain the safety constraint. The pressure sensor should send a signal to the logic controller when the pressure is high, and the logic controller should give a command to the pressure relief valve to reduce pressure. The pressure relief valve should work accordingly. An alternative controller should also work in case of the regular controller does not work. If any of the controllers cannot function as designed or as it should be, hazard occurs. The next step is to find the necessary control actions to maintain safety constraints.

3.4. Identification of required control actions to keep the system safe

As discussed in the previous section, accidents in complex system evolve from unsafe or inadequate control actions by automatic or human controllers. Risky control actions can be provided due to incorrect or missing feedback or due to miscommunication between multiple controllers.

STPA defines four types of unsafe, hazardous control actions as following: (Leveson, 2004):

1 An action required for safety is missing; e.g., the operator does not close the intake valve when the storage tank is full.
2 An unsafe control action occurs, e.g., the operator opens the intake valve when the storage tank is full.
3 A potentially safe control action occurs too early or too late than the required time, e.g., a thermal relief valve is opened too late after detection of high temperature.
4 A required safe control action is stopped too soon or applied too long (Leveson, 2004), e.g., a thermal relief valve is closed too quickly before reducing the temperature to a safe level.

3.5. Identification of low-level contribution factors or scenarios

After the identification of potentially unsafe control actions, the next step is to determine how these risky control actions can occur or how the dangerous situations can evolve that can lead to a precarious system state or accident. This step identifies the scenarios, where safe control actions are not executed correctly, perhaps because of a component failure in the controlled process.

The primary goal of any hazard analysis is to identify hazards so that they can be eliminated or prevented or mitigated which the system cannot avoid. This goal can be achieved entirely by identifying the constraints underlying the hazardous scenarios identified by hazard analysis. During the construction of a safety control structure, all entities, along with their responsibilities, should be considered to establish the safety constraint. The control structure diagram shows the connections. For example, chief engineer of the plant is responsible for technical standards and system safety requirements and all changes, variances, and waivers to the conditions. The control actions assigned to the chief engineer are:

- To monitor the activities whether they are carried out following technical standards and policy
- To establish the technical requirements and to ensure that they are enforced and implemented in the projects

The control structure should consider all his responsibilities to ensure that the design is compliant with the requirements. When the chief engineer cannot perform all the duties alone, he has the responsibility to ensure that other responsible persons in the plant do the job. Duties of all responsible entities should be carefully considered to check the necessary control actions. When multiple people or groups control the same process, coordination risk arises. The types of unsafe interactions that may result include: (1) both controllers assume that the other is performing the control responsibilities and, as a result, nobody does, or (2) controllers provide adverse control actions that have unintended side effects. When the system requires the assignment of similar duties to multiple controllers, indicator program includes the constraints of coordinating the activities.

3.6. Identification of the safety performance indicators

The required control actions identified in the previous step provide input to the safety indicator identification. The present

step identifies possible safety indicators from safety constraints. The indicators reflect the performance of the associated subsystems. One or several indicators can be identifiable for each constraint. During the development of indicators, one should focus on the properties of the system (e.g., dangerous substances, failures in the organizational structure). Indicators follow the topic of two categories. The first category includes indicators for the technical elements considered. The second category includes organizational elements. During the indicator identification, analysts consider the existing organizational structure of the organization and responsibilities of each entity. The flexibility of the organizational structure, robustness (communication between actions), resourcefulness (adequate system), decision support (proper decision support system) and redundancy (redundancy in information processing) affect the identification of indicators.

Following topics influence the consideration of indicators:

- Operability: How the organization can keep the equipment or system in a safe and reliable functioning condition, according to pre-defined operational requirements.
- Design and engineering: Required constraints in designing functional products and processes.
- Training and competence: Training and competence necessary to develop among the organization to operate the system smoothly
- Human resource management: Strategic approach to the effective management of workers of the organization so that they contribute to achieving the overall goal regarding safety.
- Audit and procurement: Requirements for audit and procurement are also important safety factors for the process industry to cover the scope of the overall system.

3.7. Development of a performance monitoring program

The plant should describe each indicator identified in the previous step thoroughly during the development of a performance monitoring program. The description should include desired safety goals, critical elements associated with the indicators, data requirements, data sources, sampling interval, indicator thresholds, and relevant references. Before the collection of data and information for the indicators, analysts should define necessary interfaces, procedures, and processes. Primary identification of indicators may result in a long list. Continuous monitoring of many indicators is time and cost consuming. Table 1 summarizes essential indicators. Threshold values are identified based on the goal of the organization. Desired safety goals reflect expected performance and achievement. Screening of the indicators depends on the frequency of update and type of operation.

Some system component may have critical safety barriers, which need frequent monitoring as every day. Indicators related to these barriers should be updated weekly or bi-weekly to identify any adverse development. On the other hand, some indicators need less frequent monitoring, e.g., periodic maintenance of check valves. The plant should not discard those indicators entirely, instead should be screened out in a separate list and overall list should be updated yearly or bi-yearly for improved safety monitoring. Existing indicators may not be relevant anymore with the modified system. List of indicators should be revised based on new hazard list or modified control action.

Determining the indicator thresholds is another challenge. For some indicators, where numbers or percentage cannot set the threshold, a level can be used to set the boundary. For example, one indicator is 'adequacy of training of operational procedure'. Level of training cannot be determined by numbers only; instead, other factors include scope of details of training, % of employees attending the training, % of employees pass the test after the training. The plant can determine a level by setting a weight for each factor. Table A.8 in the Appendix shows an example. For these indicators, low, medium, and high, are proposed as classes or limits. L̈ow, for example, means that the safety threshold is very close to being violated, whereas ḧighm̈eans that the safety performance is excellent. For each safety indicator, the plant should define such thresholds individually. Facilities can set their target value based on practicality, target risk level, the additional cost to reach the target, authority requirement, and vice versa. A target value is, for example, in the oil-gas industry SIL 2 rating of critical safety equipment is acceptable. SIL 1 is not acceptable, and working hours should not exceed 1800 h per year, 40 h per week for onshore.

4. Case study

4.1. Defining the scope of the case study

The present paper has chosen an LNG Floating Storage and Regasification Unit (FSRU) as a case study. Due to the advantages of flexibility and economy of production of LNG, LNG FSRU has attracted more attention in recent years. One of the benefits of the FSRU is that it is movable, which provides increased operational flexibility. The offloading system is an essential part of FSRU. The function of this system is to transport the LNG from the LNG carrier to an FSRU. Since the regasification process and storage conditions are the same in all setups, they differ mainly in the application of specific technologies to some pieces of equipment. Commonly, the offloading system is mountable in the stern or middle of FSRU, which consist of supporting structure, joints, and pipeline. There are several concepts to carry this offloading operation. Before starting the analysis, analysts should observe each parameter influencing the transportation systematically. As a cryogenic liquid, LNG is entirely different from oil and LPG. It is sensitive to changes in temperature and pressure and incident to vaporize. Heated or decompressed LNG generates boil-off gas. It is a waste of LNG and will also affect the offloading process and damage the pipeline.

4.1.1. Description of system boundaries and the control structure of the system

LNG carriers ship LNG as a cryogenic liquid at about -160 C. At the terminal, LNG is transferred by unloading arms to the storage tank for storage at the same cryogenic conditions as in the carrier ($-160\,^{\circ}C$ and pressure slightly above the atmospheric). Boil off Gas (BOG) management represents an essential aspect of the terminal. During LNG unloading operations, the BOG is transferred to the ship by the BOG return arm, to avoid vacuum depressurization of carrier tanks.

The main component of the transfer process is the pump. Other parts include control valves, hoses, pipelines. Valves are used to control the nature of the flow, e.g., pressure, temperature, flow rate. Emergency relief valves or couplings can stop the operation or disconnect the pipes to abort the operation in case of an emergency. Fig. 1 in the Appendix shows a simplified process flow diagram. Top filling of the receiving tank is commonly used to reduce the pressure in the tank. To start the transfer from tank one to tank two, valves V3, V4, V7, V8, V11, V12, and V15 should be opened.

Fig. 2 in Appendix shows the high-level safety control structure of the STS transfer operation, where several agencies (LNG carrier authority, floating storage and regasification plant authority, and terminal authority) are involved in safety oversight of the operation. Each component in the control structure can control the behavior of some lower level components in the structure. The present system has three types of controllers, which are logic controller, control room operator, and the site operator. Controllers conduct the operation, maintaining safe operational limit

Table 1
Summary of indicators developed by the STAMP method.

Topic		Indicators	
1	Mechanical integrity	1	Level of the reliability of all critical safety equipment including valves and sensors
		2	Percentage of shutdown/isolation systems that functioned to the desired performance standard when tested
2	Documentation and procedure	3	Adequacy of documentation on emergency response action, accident investigation, OSH policies
		4	Percentage of documented history data on equipment and maintenance actions plan
		5	Adequacy of documentation on the management of change, organizational changes, change of procedure or equipment including authorization check, post-change check
3	Human resource management	6	Level of competency of personnel for corrosion check, debris check, emergency preparedness, OHS related duties, product transfer, auditing
		7	No of extended shifts per local operators, supervisors, and managers during the measurement period
4	Inspection, maintenance, and audit	8	Level of inspection in a year on safety critical instruments, emergency response system, vessel, pipe wall
		9	No of corrective and preventive actions initiated and carried out because of the audit
		10	Level of detail of risk analysis (no of incidents identified, no of unacceptable risk issues)
5	Risk assessment	11	Percentage of risk reduction actions achieved
		12	No of corrective and preventive actions carried out because of root cause analysis of the work-related accident, diseases, and incidents
6	Training and competence	13	Level of training on emergency rescue action, product transfer, root cause analysis, operational procedure, parameter, automation, corrosion check, prevention, product quality check, change of procedure, auditing
7	Work permit system	14	Level of documentation on work permit issues including the period for completing the task along with hazards, risks and control measures

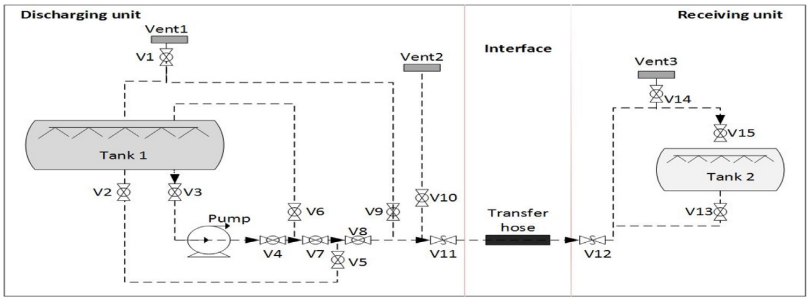


Fig. 1. Process sketch of LNG ship to ship transfer procedure.

by providing an appropriate command to the actuator system. The actuation system of the present system are pumps, non-safety valves, thermal relief valves, emergency relief coupling, and emergency shut down valve (Fig.1).

4.2. Identification of system level hazards, accidents, and safety constraint

The present paper identifies accident scenarios through the application of the STPA method. For a processing system like a present case study, leak, or fluid discharge in the system carries the principal risk of the containment. A leak in the system may lead to further accidents like Fire, Explosion, Human Injury, Loss of Containment. Therefore, this unexpected event is given the most priority in the present study, and analysis is carried out based on this. High-level system hazard related to this unexpected event is high pressure, temperature, flow rate, the liquid level in the system. Other system related hazards include corrosion, the impurity of product and external hazard includes high wind, wave, or dropped object. Hazard lists depend on the equipment type, material properties, operating condition, and physical state of the handled substances. The present case study deals with a long pipe during unloading from a ship tanker. Safety constraints are, therefore, to keep the temperature, pressure, flow rate, liquid level of the system below the threshold limit. Other safety constraints are to protect the system from corrosion and keep the system safe form high wind, wave, or dropped object. This paper does not consider secondary damages (loss of production, impact on reputation, compensations, and files).

4.3. Identification of required control actions to keep the system safe

Hazardous control actions are identified (Table A.3 in Appendix) by considering each generic mode of unsafe control actions. In this case, one hazard is high pressure in the pipe system, which is controllable by activating a pressure relief valve. The control action here is Äctivate Pressure Relief Valve (PRV)ı. This action can be done by a logic controller, a control room operator, or site operator after getting feedback from the pressure sensor. Logic controllers can automatically activate the PRV when the pressure is high. A control room operator can also act as a controller if the logic controller cannot act on time or may notify the site operator to activate the valve manually. To execute these processes safely, sensors, valves, the logic controller, electricity and site operators must be available, and function/act as intended. Primary causes concern maintenance, quality, safety culture, personnel competence.

4.4. Determination of corrective actions to rectify the dangerous causes

This step is performed to determine how low-level hazard can be eliminated or prevented. This step identifies scenarios and causal factors relating to why and how hazardous control actions can occur (Table A.3 in appendix). After determining the low-level causal situations, all possible mitigating measures are sought to reduce or mitigate the hazard. For example, to ensure that pressure and temperature do not exceed a defined limit in the system, thermal relief valves work correctly. This requirement can be secured by design-

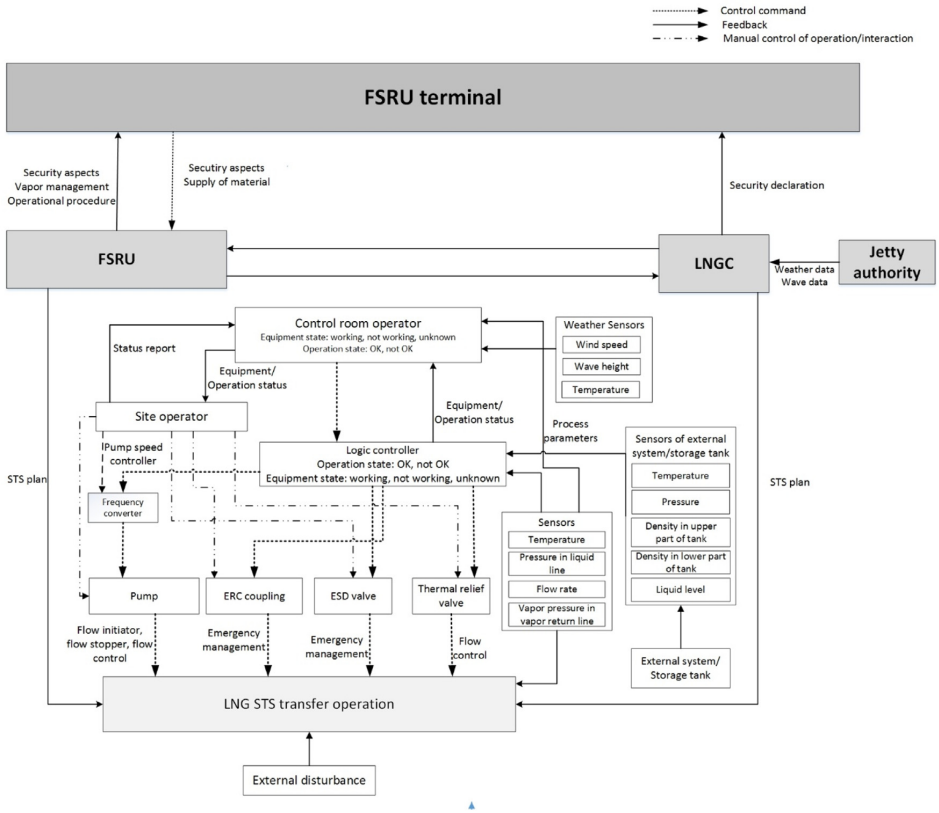


Fig. 2. Control structure of LNG STS transfer.

ing all valves and sensors to comply with industry design standards and codes and by maintaining them properly.

4.5. Identification of safety performance indicators

Indicators are identified based on previously developed safety constraint. When defining the indicators from the safety constraints, the focus is given first to the design possibilities, second to maintenance actions, and after that training, competence, and other issues. For example, one safety constraint is that an instrument or equipment should comply with current design standards and codes. This constraint is related to the design performance. The identified indicators are the "% of safety critical items of the plant or equipment which comply with specified design standards". The next step is to define the unit and target values of those indicators. If the indicator value is less than the desired value, necessary actions need to be taken, e.g., replacing critical safety items.

The plant should define the threshold value for each indicator. Depending on the nature of the indicator (whether it is a p̈ositiveör a n̈egativeïndicator), the target may be to exceed or go below the threshold. An example may be the two indicators ẗhours of safety training per person per yeaänd äverage percentage of right answers in the test.̈ If the plant reaches the target ẗhours of training ,̈ but the äverage percentage of right answers in the testsïs below target, the analyst can conclude that the plant should increase the quality of training rather than increasing the number of hours. Sequences of identification of safety indicators:

4.6. Development of a performance monitoring program

The resulting list contains 56 indicators (Table A.3), which is a high number considering the limited system. Most of the indicators do not require continual assessment. Table 1 summarizes indicators separately which need continuous reviewing (e.g., Percentage of periodically verified OSH requirements applied to purchase specifications of machinery, equipment, and others; no of maintenance checks of emergency equipment regularly, Percentage of indicators subject to periodic review and update). This paper identifies fourteen indicators (Table 1) as requiring a regular update (Fig. 3).

One indicator is 'Adequacy of documentation'. Ädequacyïeeds to be specified and defined in such a way that it can be measured. Examples can be the proportion that is in written form, accessibility by operators and managers and readability. Another indicator is 'Adequacy of training'. The plant can specify this adequacy by considering whether the training covers all or specific aspect, % of employees participating in the training and % passing the test after doing the course. After reaching the predefined targets, the company might define more ambitious goals.

The review of safety performance should be a process of continuous improvement. Indicators are a tool for regular (e.g., monthly) evaluation of the condition. This statement does not mean that performance indicators are a replacement for an audit system. Instead, it is a complementary activity of more frequent reviewing that enables faster detection of weaknesses and subsequent intervention. Indicators may also be developed and used at all levels in an organization, such as top management, business area, facility, or

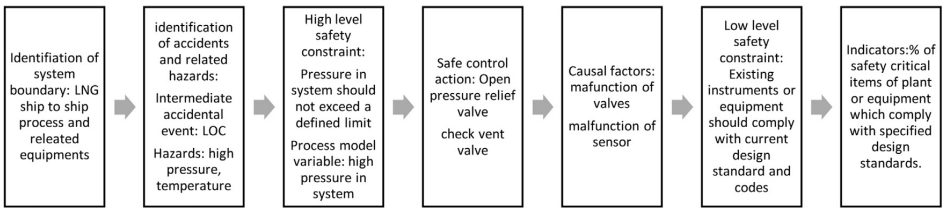


Fig. 3. Identification of indicators in the system engineering approach.

specific activity. However, the same indicators are not necessarily useful at all levels. Thus, the indicators need to be meaningful at the level where they primarily are being aimed. Indicators developed for the use of operational management should be relevant for that level, even if this does not necessarily mean to be useful and relevant for higher levels in the organization.

5. Development of OECD and CCPS indicators

The present paper develops indicators by the method described in the OECD guideline and CCPS guideline (presented in Table A.4 to Table A.7 in Appendix) to do a comparative analysis between STAMP based performance indicators and indicators developed by those methods. The paper develops outcome and activities indicators for the plant according to OECD guidelines.

OECD guidance does not define a precise method but provides advice on how to develop and use safety performance indicators. The guidance defines two types of indicators: activities indicators and outcome indicators. Activities indicators help the organization to check whether they are taking actions in lowering risk. Outcome indicators help to check whether such effects are leading to less likelihood of an accident or to reduce the adverse impact on human health or the environment from an accident. It can also develop an understanding of established or achieved goals by law/regulation, corporate policies, or community objectives. Thus, the guidance provides a tool for prioritization and a basis for improving the effectiveness of spending on safety-related expenditures and allocation of human and other resources.

It has been decided to review all the chapters of part A of the guidance document and to determine which subchapters are relevant for their purposes. Present work included six sections from outcome indicators, which are general management of safety, administrative, technical issues, emergency preparedness, and accident reporting seems to be relevant for LNG FSRU. Some of the indicators are straightforward to measure. For each of the indicators, parameters are established to be understood by all the employees. The company can apply a scale for the assessment of outcome indicators from 1 to 10, with 10 being the best performance.

In the present case, the team has decided to use a weighting system to place greater emphasis on those parameters that are of more considerable significance. Table A.8 in Appendix shows an example. One hundred outcome indicators are developed to check whether the plant has achieved the desired result in establishing a proper safety management system. If these indicators show poor results, a related activities indicator should be evaluated to ensure that the issue is focused appropriately. Present case study develops thirty-eight activities indicators.

The present case develops CCPS lagging and leading indicators. ĽaggingЌetrics are a retrospective set of metrics based on incidents that meet the threshold of severity as part of the industry-wide process safety metric. Leading metrics indicate the efficiency of the safety management system and give an early indication of deterioration in the effectiveness of these critical safety systems and enable remedial action to be undertaken to restore the effectiveness of these essential barriers before any loss of containment event takes place.

CCPS's metrics consider Tier 1 process safety incident depending on process involvement, above the minimum reporting threshold, location, and acute release. The term 'Process' is used here only for equipment and technology used for chemical or petrochemical products, including tanks, pipe, or condensation system (CCPS, 2007). Tier 1 incidents are an unplanned or uncontrolled release of any material including not toxic and non-flammable materials from a process which causes severe consequences like employee injury or fatality or evacuation or fire or explosion and release of the toxic substances above a defined threshold. An incident where there is no direct chemical or process involved is not accountable as a process safety incident. For example, fire in an office building will be not reported as a process safety incident if the fire does not occur from a chemical reaction or process incident (CCPS, 2007). This criterion intends to identify those incidents that are related to process safety, as distinguished from personal safety incidents that are not process-related.

A "1-h" rule (amount of material releases to same or above a predefined threshold in 1 h) applies to Tier 1 incidents. Tier 2 Process Safety Events represents those LOPC incidents with a lesser consequence than a Tier 1 PSI. A Tier 2 LOC is an unplanned release of non-toxic or non-flammable material including steam, hot condensate, compressed CO2 or compressed air with lesser consequences and was out of scope in Tier 1. Process Safety Total Incident Rate (PSTIR) is the cumulative (annual) count of incidents normalized by man-hours. Process Safety Incident Severity Rate (PSISR) is the cumulative (annual) severity-weighted rate of process safety incidents. Developed leading metrics for the safety systems are Maintenance of mechanical integrity; Action items follow-up; Operating and Maintenance Procedures, Process safety training and competency, and Fatigue risk management.

Mechanical integrity metric is one measure of the effectiveness of the process safety management system to ensure that safety-critical plant and equipment is functional. This metric involves collecting data on the delivery of planned inspection work on safety critical plant and equipment. The calculation of the metric determines the number of inspections of safety critical plant and equipment planned for the measurement period.

'Action item follows up' metric determines the number of inspections of safety critical plant and equipment completed during the measurement period (CCPS, 2007). This metric is to determine how effectively the plant can fix identified deficiencies of process safety equipment on time. 'Process safety training and competency' metric provides a mechanism for measuring the effectiveness of process safety culture within chemical process organizations.

'Operating & Maintenance Procedures' metric measures the progress of necessary maintenance procedures during the specified period. This metric may include a huge list of criteria for monitoring, for example, action steps that are clear and adequately ordered, consequences of deviation from boundaries, steps to maintain the safe limit, checklists (where appropriate). Fatigue risk management

metric helps to reduce fatigue risk for employees. It monitors the organization's activity to manage fatigue risk, for example, no of time in employee training, no of safety meetings and like.

The present case study develops a total of 17 lagging and 14 leading indicators relevant to the STS operation.

6. Discussion

This paper has defined safety indicators following a system engineering approach. The present paper selects LNG ship to ship transfer process as the case study without specifying specific process parameters. Developed indicators can measure safety at the conceptual design stage. STPA can be started in early concept analysis to assist in identifying safety requirements and constraints. The method can cover possible causal scenarios of accidents including accident prevention design technique, redundancy, barriers, human intervention, use of operational procedures, checklists, and training in the analysis. Scenarios can be used to create additional requirements, including mitigation or new design decisions. A benefit of STAMP is that is can be easily modified or revised for any change of plant or system component. For any change, one needs to find the associated hazards, safety constraints, and controller actions and then develop the performance indicators accordingly.

The overall goal is to prevent major accidents and to establish an effective safety management system. It is essential to check whether this safety management system can cope with the risks involved and whether it works well. Although the primary link between safety management and safety performance in hindsight, lessons learned from accidents address failures in the safety management system, for example, BP Texas City accident.

STAMP indicators are developed from a control hierarchy diagram and give an abstract of how a dangerous scenario can occur and what safety constraints should be enforced to avoid the hazard. It considers both leading and lagging indicators at the same time. One practical problem related to this model is that it develops a high number of indicators in the first stage. To choose the important indicators from this list is a challenging task. Regarding getting early warning signals, STAMP is very useful, as it can identify even a valve failure or low audibility problem immediately. So, STAMP can identify errors at the root level. Instantaneous identification of flaws in the plant is possible, and so the plant can rectify them quickly. The plant can use threshold values as early warning criteria.

The developed indicators are said to be a mix of leading and lagging indicators. Indicators are leading in the sense that they are giving importance to proactive action before any occurrence of accidents, for example, no of inspection and maintenance checks of shutdown system and no of existing procedures with the proper scope and enough detail. Some indicators are also developed based on previous operational records to check missing barriers in operational processes or systems. Those indicators are comparable as lagging indicators, for example, no of reported flaws in the automated system and no of stated incorrect parameters by operators. A leading indicator-based system can monitor the effectiveness of the control system, can improve safety performance and can, therefore, reduce exposure to the risk of having an accident or serious incident. an effective PMS system can monitor past performance and can help to plan future performance (Medina-Herrera et al., 2014)

Development of indicators from safety constraints is quite challenging. For example, one constraint is that an operator should be aware of the correct operational procedures. What are the control actions to measure that an operator is aware of the proper procedures and can implement them incorrectly? It can be training programs to operators, internal quiz or test to check the competency of the operator, and correct documentation which the operator can follow. However, one may still ask if this is enough. Monitoring of indicators established by the present method is quite simple; however, it may become profoundly human resource intensive.

Indicators based on STAMP are plant-specific while the OECD guidance has predefined sets of indicators. It gives quite an extensive collection of indicators, especially in hazard management and personnel safety management. The STAMP-based method focuses mainly on operational indicators because it has a clear link to unexpected events that the company wants to avoid. The causal chain of an unexpected event can identify all relevant organizational issues. However, in the case study, the problem is that the system is relatively limited and does not include the whole organization required to operate it.

The present approach supports continual improvement and emphasized achievements rather than failures. It is possible to express the status of the indicator in a way to record and to compare with previous and future results. It is possible to classify the status into different categories (e.g., high/medium/low, grade A–F). Be cost-effective in terms of data collection: the effort of gathering data for the indicator not is too excessive compared to benefits gained by using the indicator. A critical criterion of indicators is comprehensibility. A link between the indicator and the factor is easy to comprehend, and the meaning of the indicator is self-evident to understand what variables to measure. It has an advantage as it measures the present status of a factor and provides an early warning that potential problems are arising. Some indicators indicate that something is wrong before the occurrence of an accident while other indicators indicate what is wrong. The present method uses a combination of both types as indicator set.

The indicator set combines more frequent indicators (e.g., monthly) with less frequent indicators (e.g., quarterly, annually, or even more seldom). Frequency can be determined based on the nature of the indicator, i.e., how often it is reasonable to assume that the status changes, but also more pragmatic criteria like usefulness and cost-effectiveness. Reason for this is that some of the factors may be constant (e.g., the design of installation), they may change only at a well-defined point in time (organization structure), or they change relatively slowly (e.g., work practice). The plant should update indicators periodically.

A critical restraint may arise from safety culture. Cultural values and assumptions affect the establishment of the safety management system. Hard and fast rules may not work in all environments or may work in exceptional cases, or may change the working environment, increase fatigue of a worker, and thereby may increase human error. Analysts should consider these issues when determining safety constraints.

In general, indicators related to work practice are difficult to monitor. They are related to the quality of work operations in many cases, and monitoring the quality of these is not easy. The present method makes it easy to track this work practice as it originates from a lack of control action by the operator and to transform it into the action list. It becomes easy to determine the required actions concerning the behavior of performance indicator and priority of the factors. It gives timely warning of deviation from safety standards of design and operation and can identify degradation in safety performance as early as possible. The plant can set a safe boundary as tolerance or targets.

One limitation is that this method does not consider any risk analysis. It cannot deduce the importance of a change in indicator values as for risk indicators. These indicators may not be suitable for benchmarking purposes because of site-specific variability. In a comparison of STAMP based method with Bayesian belief network, the process of developing KPI using Bayesian belief network (Gerbec and Kontić, 2017) requires consideration of direct fail-

ures, as well as of factors affecting the events and probabilities and relationship with essential safety indicators. A benefit of using the BBN model is that the level of risk can be quantified. Level of risk reduction by implementing technological and organizational means becomes quantifiable also.

It is said that a system-based model can better deal with system uncertainty (Kazaras et al., 2012). Events are comparable as control action and control flaws are the consequences; the next step is ranking them in terms of uncertainty. How uncertain of such an 'event' to occur depends mainly on the uncertainty of the safety control measure responsible for controlling the causal event. The second question is about the validity and reliability of the analysis. Several researchers (Johnson and de Almeida, 2008; Katsakiori et al., 2009; Salmon et al., 2012; Underwood and Waterson, 2014) have worked on the comparative study of system-based analysis with other models. Filho et al. (2018) compared the validity of STAMP method with other models for a ferry accident. Fault tree analysis and event tree analysis are well known and widely applied to the industry which proved their validity. System based model gives additional coverage of organizational significant picture information (Branford, 2011). Such big picture is often missing in a traditional method.

CCPS lagging indicators consider tier 1 process safety incidents with high consequences and tier 2 process safety events with lesser consequences. CCPS defines industry process safety metrics, so it is easier to make a comparison of incidents in different years and how the plant is running concerning safety. CCPS leading indicators give focus to mechanical integrity; action items follow up, process safety training, operating and maintenance procedure, and fatigue risk management. Safety management systems developed from CCPS safety indicators give a complete overview of the plant with low effort and cost compared to OECD and STAMP indicators. Tier 2 lagging indicators should be given focus to consider early warning signs.

The STAMP model is better than OECD and CCPS concerning potentiality for early warning, the area of focus, level of details of the study, the possibility to focus on specific issues and ease of modification of model for a change in the system. However, this model is still new, and industry personnel does not have expertise in how to use it. Low-level hazards which do not belong to any class of unexpected event and hazardous control actions may have fallen outside the scope of analysis. The analysis should include actors, preconditions, alternative processes, and non-functional requirements to improve the sophistication of the study. More study can be done in the future to enhance the screening stage to achieve enough control with a lower number of indicators. Indicators serve as a tool for regular monitoring of the condition of factors. Indicators are not a replacement for an audit system. Instead, it is a complementary activity of control which allows for faster intervention to improve the condition. Indicators can be developed and used at all levels in the organization such as top management, business area, facility, or specific activity.

7. Conclusion

This paper presents a method for the development of safety indicators based on system engineering. The paper has dealt with three main tasks. The first task is the development of a technique for system-based safety indicators, the second task is to apply this to a case study, and the third is to make a comparison between the developed method and previously established methods (OECD and CCPS). The paper uses the STAMP accident model. The analysis shows that STAMP-based modeling provides a better understanding of the system. The STAMP-based indicator development process helps to focus on specific issues from which a hazard can evolve. It takes into consideration human and organizational factors along with technical elements to mitigate or prevent high level as well as low-level system hazards. Another benefit is that STAMP based indicators can easily be modified or revised for any change of plant or system component. The third part of the analysis presents a comparative study between a STAMP-based indicators program and indicators developed by the methods described by OECD and CCPS. OECD gives an extensive set of indicators, especially in hazard management and personal safety management. It seems that STAMP based model takes much effort to enable the control hierarchy and rest procedures. However, compared to the diversity of the method and detail of the analysis, the amount of effort is worth. STAMP based modeling provides a better understanding of the system compared to other analysis. Future work can be an integration of any risk quantification model with the STAMP model. This integration will support the screening of indicators. Further work is also necessary to investigate to what degree these system engineering-based indicators are complementary to other safety performance indicators or whether they provide a more appropriate measure to foresee unexpected occurrences.

Acknowledgments

The authors wish to thank the Norwegian Research Council and DynSoL AS for their financial support for this project through project number 283861. The contribution of project team members Gisle Obrestad and Kamrul Islam is also acknowledged.

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:https://doi.org/10.1016/j.psep.2019.05.047.

References

Ale, B., 2009. More thinking about process safety indicators. Saf. Sci. 47, 470–471.
Baker, J., Bowman, F., Erwin, G., Gorton, S., Hendershot, D., Leveson, N., Priest, S., Rosenthal, I., Tebo, P., Wiegmann, D., 2007. The Report of the BP US Refineries Independent Safety Review Panel, 2007. BP, US.
Basso, B., Carpegna, C., Dibitonto, C., Gaido, G., Robotto, A., Zonato, C., 2004. Reviewing the safety management system by incident investigation and performance indicators. J. Loss Prev. Process Ind. 17, 225–231.
Bellamy, L., 2012. A literature review on safety performance indicators supporting the control of major hazards, RIVM report, National Institute for the Public Health and the Environment, Dutch Ministry of Health. Welfare and Sport.
Benner, L., 1975. Accident investigations: multilinear events sequencing methods. J. Safety Res. 7, 67–73.
Branford, K., 2011. Seeing the Big Picture of Mishaps. Aviation Psychology and Applied Human Factors.
Ccps, A., 2007. Guidelines for Risk-based Process Safety. N.J.: Wiley-Interscience, Hoboken.
Clarke, S., 2006. The relationship between safety climate and safety performance: a meta-analytic review. J. Occup. Health Psychol. 11, 315.
Csb, M., 2007. Investigation Report: Refinery Explosion and Fire. BP Texas City Incident Final Investigation Report.
Davoudian, K., Wu, J.-S., Apostolakis, G., 1994a. Incorporating organizational factors into risk assessment through the analysis of work processes. Reliab. Eng. Syst. Saf. 45, 85–105.
Davoudian, K., Wu, J.-S., Apostolakis, G., 1994b. The work process analysis model (WPAM). Reliab. Eng. Syst. Saf. 45, 107–125.
Embrey, D.E., 1992. Incorporating management and organizational factors into probabilistic safety assessment. Reliab. Eng. Syst. Saf. 38, 199–208.
Epri, 2000. Guidelines for Trial Use of Leading Indicators of Human Performance: The Human Performance Assistance Package. Electric Power Research Institute, Palo Alto, CA: U.S.
Epri, 2001. Final Report on Leading Indicators of Human Performance. Washington, DC: EPRI. Palo Alto, CA, and the U.S. Department of Energy, Washington, DC.
Erikson, S.G., 2009. Performance indicators. Saf. Sci. 47, 468.
Filho, A., Jun, G., Waterson, P., 2018. Four studies, two methods, one accident-An examination of the reliability and validity of Accimap and STAMP for accident analysis. Saf. Sci. 113, 310–317.
Forest, J.J., Kessler, K., 2013. Correlating process safety leading indicators with performance. Process. Saf. Prog. 32, 185–188.

Gerbec, M., Kontić, B., 2017. Safety-related key performance indicators for securing long-term business development–A case study. Saf. Sci. 98, 77–88.

Gibson, J.J., 1961. The contribution of experimental psychology to the formulation of the problem of safety–a brief for basic research. Behav. Approach. Accid. Res. 1, 77–89.

Gómez-Cobo, A., 2002. Indicators to Monitor NPP Operational Safety Performance. International Atomic Energy Agency, Department of Nuclear Safety, Austria.

Grabowski, M., Ayyalasomayajula, P., Merrick, J., Mccafferty, D., 2007. Accident precursors and safety nets: leading indicators of tanker operations safety. Marit. Policy Manag. 34, 405–425.

Grote, G., 2009. Response to andrew hopkins. Saf. Sci. 47, 478.

Guastello, S.J., 1993. Do we really know how well our occupational accident prevention programs work? Saf. Sci. 16, 445–463.

Guo, B.H., Yiu, T.W., 2015. Developing leading indicators to monitor the safety conditions of construction projects. J. Manag. Eng. 32, 04015016.

Haddon Jr, W., 1968. The changing approach to the epidemiology, prevention, and amelioration of trauma: the transition to approaches etiologically rather than descriptively based. Am. J. Public Health Nations Health 58, 1431–1438.

Hale, A., 2009. Why safety performance indicators? Saf. Sci. 47, 479–480.

Haugen, S., Seljelid, J., Nyheim, O., Sklet, S., Jahnsen, E.A., 2012. Generic method for identifying major accident risk indicators. In: 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference., pp. 5643–5652.

Haugom, G., Friis-Hansen, P., 2011. Risk modelling of a hydrogen refuelling station using Bayesian network. Int. J. Hydrogen Energy 36, 2389–2397.

Heinrich, H., 1931. Industrial Accident Prevention: A Scientific Approach. McGraw Hill, New York.

Herrera, I.A., Hollnagel, E., Håbrekke, S., 2010. Proposing safety performance indicators for helicopter offshore on the Norwegian continental shelf. In: PSAM 10-Tenth Conference on Probabilistic Safety Assessment and Management., pp. 10.

Herrera, I., Hovden, J., 2008. Leading Indicators Applied To Maintenance In The Framework Of resilience engineering: a conceptual approach. In: The 3rd Resilience Engineering Symposium., pp. 30.

Hinze, J., Thurman, S., Wehle, A., 2013. Leading indicators of construction safety performance. Saf. Sci. 51, 23–28.

Hollnagel, E., 2017a. FRAM: The Functional Resonance Analysis Method: Modelling Complex Socio-technical Systems. CRC Press.

Hollnagel, E., 2017b. Resilience: the Challenge of the Unstable. Resilience Engineering. CRC Press.

Hollnagel, E., Woods, D.D., 2006. Epilogue: resilience engineering precepts. Resilience Engineering: Concepts And Precepts, 347–358.

Holmberg, J., Söderlund, T., Forss, A., Gunsell, L., 1998. Operating experience feedback by risk-based PSA-indicators; Safety and reliability. In: Proc. of the European Conference on Safety and Reliability—ESREL., pp. 16–19.

Hopkins, A., 2000. Lessons From Longford: the Esso Gas Plant Explosion. CCH Australia Ltd.

Hopkins, A., 2008. Failure to Learn: the BP Texas City Refinery Disaster. CCH Australia Ltd.

Hopkins, A., 2009. Thinking about process safety indicators. Saf. Sci.

Hse, 2006. Developing Process Safety Indicators—A Step-By-Step Guide for Chemical and Major Hazard Industries. Health and Safety Executive, UK.

IAEA, 2000. Operational Safety Performance Indicators for Nuclear Power Plant. IAEA, Austria.

Jablonowski, C.J., 2012. Identification of leading safety indicators in onshore oil drilling. Energy Explor. Exploit. 30, 523–532.

Johnson, C.W., De Almeida, I.M., 2008. An investigation into the loss of the Brazilian space programme's launch vehicle VLS-1 V03. Saf. Sci. 46, 38–53.

Katsakiori, P., Sakellaropoulos, G., Manatakis, E., 2009. Towards an evaluation of accident investigation methods in terms of their alignment with accident causation models. Saf. Sci. 47, 1007–1015.

Kazaras, K., Kirytopoulos, K., Rentizelas, A., 2012. Introducing the STAMP method in road tunnel safety assessment. Saf. Sci. 50, 1806–1817.

Khan, F., Abunada, H., John, D., Benmosbah, T., 2010. Development of risk-based process safety indicators. Process. Saf. Prog. 29, 133–143.

Khawaji, I., 2012. Developing System-Based Leading Indicators for Proactive Risk Management in the Chemical Processing Industry Thesis. MIT, June.

Kjellén, U., 2000. Prevention of Accidents Through Experience Feedback. CRC Press.

Kjellén, U., 2009. The safety measurement problem revisited. Saf. Sci. 47, 486–489.

Knijff, P., Allford, L., Schmelzer, P., 2013. Process safety leading indicators—a perspective from Europe. Process. Saf. Prog. 32, 332–336.

Körvers, P., Sonnemans, P., 2008. Accidents: a discrepancy between indicators and facts! Saf. Sci. 46, 1067–1077.

Laakso, K., Holmberg, J., Lehtinen, E., Johansson, G., 1994. Safety Evaluation by living probabilistic safety assessment and safety indicators. Nordisk Ministerraad.

Leveson, N., 2004. A new accident model for engineering safer systems. Saf. Sci. 42, 237–270.

Leveson, N., 2015a. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34.

Leveson, N., 2015b. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34.

Lingard, H., Hallowell, M., Salas, R., Pirzadeh, P., 2017. Leading or lagging? Temporal analysis of safety indicators on a large infrastructure construction project. Saf. Sci. 91, 206–220.

Mearns, K., 2009. From reactive to proactive–Can LPIs deliver? Saf. Sci. 47, 491–492.

Mearns, K., Whitaker, S.M., Flin, R., 2003. Safety climate, safety management practice, and safety performance in offshore environments. Saf. Sci. 41, 641–680.

Medina-Herrera, N., Jiménez-Gutiérrez, A., Mannan, M.S., 2014. Development of inherently safer distillation systems. J. Loss Prev. Process Ind. 29, 225–239.

Mogford, J., Texas City, Texas, USA, 9, 2005 2005. Fatal Accident Investigation Report. Isomerization Unit Explosion Final Report.

Murphy, D.M., Paté-Cornell, M.E., 1996. The SAM framework: modeling the effects of management factors on human behavior in risk analysis. Risk Anal. 16, 501–515.

Nelson, P.F., Martin-Del-Campo, C., Hallbert, B., Mosleh, A., 2016. Development of a leading performance Indicator from operational experience and resilience in a nuclear power plant. Nucl. Eng. Technol. 48, 114–128.

Nielsen, L., Sklet, S., Oien, K., 1996. Use of risk analysis in the regulation of the Norwegian petroleum industry. Proceedings of the Probabilistic Safety Assessment International Topical Meeting, 756–762.

Oecd, 2003. Oecd Guidance on Safety Performance Indicators: A Companion to the OECD Guiding Principles for Chemical Accident Prevention, Preparedness, and Response. Organisation for Economic Co-operation and Development, Paris.

Øien, K., 2001a. A framework for the establishment of organizational risk indicators. Reliab. Eng. Syst. Saf. 74, 147–167.

Øien, K., 2001b. Risk indicators As a tool for risk control. Reliab. Eng. Syst. Saf. 74, 129–145.

Øien, K., 2008. Development of Early Warning Indicators Based on Incident Investigation. Sintef, Trondheim, Norway.

Øien, K., Massaiu, S., Tinmannsvik, R., Størseth, F., 2010. Development of early warning indicators based on resilience engineering. Submitted to PSAM10, International Probabilistic Safety Assessment, and Management Conference, 7–11.

Øien, K., Sklet, S., 1999. Application of Risk Analyses in the Operating phase, Establishment of Safety Indicators, and Modelling of Organizational Factors' Effects on the Risk Level–A 'State-of-the-art'. *STF38 A99416*. SINTEF Technology and Society, Safety Research, Trondheim, Norway.

Øien, K., Sklet, S., Nielsen, L., 1997. Risk level indicators for surveillance of changes in risk level. In: Proceedings of ESREL., pp. 1809–1816.

Øien, K., Sklet, S., Nielsen, L., 1998. Development of risk level indicators for a petroleum production platform. Proceedings of the 9th International Symposium of Loss Prevention and Safety Promotion in the Process Industries, 4–7.

Øien, K., Utne, I.B., Herrera, I.A., 2011. Building safety indicators: part 1–theoretical foundation. Saf. Sci. 49, 148–161.

Paltrinieri, N., Øien, K., Cozzani, V., 2012. Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. Reliab. Eng. Syst. Saf. 108, 21–31.

Papazoglou, I.A., Bellamy, L.J., Hale, A.R., Aneziris, O.N., Ale, B.J.M., Post, J.G., Oh, J.I.H., 2003. I-Risk: development of an integrated technical and management risk methodology for chemical installations. J. Loss Prev. Process Ind. 16, 575–591.

Pasman, H.J., Knegtering, B., Rogers, W.J., 2013. A holistic approach to control process safety risks: possible ways forward. Reliab. Eng. Syst. Saf. 117, 21–29.

Paté-Cornell, M.E., 1993. Learning from the piper alpha accident: a postmortem analysis of technical and organizational factors. Risk Anal. 13, 215–232.

Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27, 183–213.

Reason, J., 1987. The Chernobyl errors. Bull. Br. Psychol. Soc. 40, 1–20.

Reason, J., 1997. Managing the Risks of Organizational Accidents. Routledge.

Reiman, T., Pietikäinen, E., 2012. Leading indicators of system safety–monitoring and driving the Organizational Safety Potential. Saf. Sci. 50, 1993–2000.

robson, L.S., Ibrahim, S., Hogg-Johnson, S., Steenstra, I.A., Van Eerd, D., Amick 3RD, B.C., 2017a. Developing leading indicators from OHS management audit data: determining the measurement properties of audit data from the field. J. Safety Res. 61, 93–103.

robson, L.S., Ibrahim, S., Hogg-Johnson, S., Steenstra, I.A., VAN Eerd, D., Amick III, B.C., 2017b. Developing leading indicators from OHS management audit data: determining the measurement properties of audit data from the field. J. Safety Res. 61, 93–103.

Rockwell, T.H., 1959. Safety performance measurement. J. Ind. Eng. 10, 12–16.

Salmon, P.M., Cornelissen, M., Trotter, M.J., 2012. Systems-based accident analysis methods: a comparison of Accimap, HFACS, and STAMP. Saf. Sci. 50, 1158–1170.

Saqib, N., Tahir Siddiqi, M., 2008. Aggregation of safety performance indicators to higher-level indicators. Reliab. Eng. Syst. Saf. 93, 307–315.

Scarponi, G.E., Paltrinieri, N., Khan, F., Cozzani, V., 2016. Chapter 7 - reactive and proactive approaches: tutorials and example. In: Dynamic Risk Analysis in the Chemical and Petroleum Industry. Butterworth-Heinemann.

Sharp, J., Ersdal, G., Galbraith, D., 2008. Development of key performance indicators for offshore structural integrity. ASME 2008 27th International Conference on Offshore Mechanics and Arctic Engineering, 123–130.

Sheehan, C., Donohue, R., Shea, T., Cooper, B., De Cieri, H., 2016. Leading and lagging indicators of occupational health and safety: the moderating role of safety leadership. Accid. Anal. Prev. 92, 130–138.

Sinelnikov, S., Inouye, J., Kerper, S., 2015. Using leading indicators to measure occupational health and safety performance. Saf. Sci. 72, 240–248.

Tarrants, W.E., 1963. An Evaluation of the Critical Incident Technique As a Method for Identifying Industrial Accident Causal Factors. New York University, School of Education.

Tarrants, W.E., 1980. The Measurement of Safety Performance. University of Michigan-Dearborn.

Thieme, C.A., Utne, I.B., 2017. Safety performance monitoring of autonomous marine systems. Reliab. Eng. Syst. Saf. 159, 264–275.

Underwood, P., Waterson, P., 2014. Systems thinking, the Swiss Cheese Model and accident analysis: a comparative systemic analysis of the Grayrigg train derailment using the ATSB, AcciMap, and STAMP models. Accid. Anal. Prev. 68, 75–94.
Vinnem, J.E., 2010. Risk indicators for major hazards on offshore installations. Saf. Sci. 48, 770–787.
Vinnem, J.E., Aven, T., Husebø, T., Seljelid, J., Tveit, O.J., 2006. Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. Reliab. Eng. Syst. Saf. 91, 778–791.
Vinnem, J., Aven, T., Sørum, M., Øien, K., 2003. Structured approach to risk indicators for major hazards. In: ESREL 2003 Conference, Maastrict, 16-18.06.
Vinnem, J., Hestad, J., Kvaløy, J., Skogdalen, J., 2010. Analysis of root causes of major hazard precursors in the offshore petroleum industry. Biometrika 97, 375–388.
Zhang, L., Wu, X., Qin, Y., Skibniewski, M.J., Liu, W., 2016. Towards a Fuzzy-Bayesian Network Based Approach for Safety Risk Analysis of Tunnel-Induced Pipeline Damage. Risk Anal. 36, 278–301.
Zhao, S., Soares, C.G., Zhu, H., 2015. A bayesian network modelling and risk analysis on LNG carrier anchoring system. Transportation Information and Safety (ICTIS), 2015 International Conference on, 432–436.

Paper VII

Sultana, S., Bucelli, M., Zhang, J., Rauzy, A., How system engineering may help prepare FMECA lesson learned from a practical case. in 28th European Safety and Reliability Conference ESREL 2018. Trondheim, Norway (Sultana et al., 2018)

Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)
© 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7

How systems engineering may be useful in preparing FMECA—lesson learnt from a practical case

M. Bucelli
Department of Civil, Chemical, Environmental and Material Engineering, Alma Mater Studiorum—University of Bologna, Bologna, Italy
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, Trondheim, Norway
Safetec, Trondheim, Norway

J. Zhang & A. Rauzy
Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology NTNU, Trondheim, Norway

S. Sultana
Department of Marine Technology, Norwegian University of Science and Technology NTNU, Trondheim, Norway

ABSTRACT: Risk communication and information exchange have become more challenging in today's complex projects, which involves different stakeholders in different roles. Unstructured data communication and flaws in knowledge exchange may lead to erroneous risk perception and evaluation. The role of risk analysis has become more critical in this perspective. This paper proposes a new way to enrich risk analysis with the help of knowledge of systems engineering. Focus is given to establish a Failure Mode, Effect and Criticality Analysis (FMECA) model using models from systems engineering which are more systematic compared to models used in tradition approach. A reference case study is analyzed, which is inspired from the subsea laboratory at the Department of Mechanical and Industrial Engineering (MTP) at the Norwegian University of Science and Technology (NTNU). The investigation focuses on the series of relevant risks for the subsea gas boosting section in offshore Oil & Gas installations. Results from the present study are discussed with emphasize on three aspects: (1) cross-system effects, (2) reasonable and reachable risk reduction measures and (3) multiple system dimension. We acknowledge that the proposed method based on system thinking can be used to construct system behavior model, which in turn could be used in FMECA development to gain better understanding of risks and to improve the overall performance of system.

1 INTRODUCTION

In the last decades, the industry, from manufacturing to chemical and Oil & Gas (O&G) sector, has become more and more complex, notably by incorporating innovative technologies requiring new stakeholders. Risk analysts are responsible for the identification and the analysis of potential risks arising from the performed activities and for treating these risks, according to established acceptance criteria (ISO 31000, 2009). Many factors affect the actual risk level in different ways. For instance, a new human machine interface may cause stress and therefore influence operator performance. The risk posed by these factors raises the importance of both the risk analyst and the communication network with the other professionals, consequently, the focus moved to risk management.

Risk management involves different disciplines at different levels across the entire enterprise. However, nowadays in the industry, the coordination between the different parties is not stressed enough when instead it should be properly maintained (Rice & Spence, 2016). Bringing different areas of expertise together in analyzing the potential risks and identify threshold criteria is still challenging. Moreover, the methods adopted for information collection and analysis are often unstructured (Kirsch, Hineb, & Maybury, 2015). The inconsistence in jargon used and the difference in the theoretical background of the different stakeholders may lead to erroneous decision-making and costly correction for inadequate and inappropriate actions.

Failure Mode, Effect and Criticality Analysis (FMECA) has been widely accepted as the risk identification and the characterization tool for

hardware components since the late 1960s. However, today's industry involves fast-moving technology innovations and faces challenging operating conditions. There is no formal procedure in constructing FMECA for such complex system and then the quality and content of FMECA depend on the competence and experience of risk analysts. In some practices, analysts start FMECA without establishing a baseline system concept. Based on this scenario, the solution is to structure coordinated and distributed system information about what is taking place and what is needed for proper risk mitigation.

The existing frameworks for risk management in Oil and Gas industry (ISO 31000, 2009; NORSOK Z-013, 2010) also highlight the needs of establishing the system concept before starting risk analysis, and maintaining and updating the system concept based on given indications, however, no detailed methods and approaches are prompted. This paper suggests the use of often-cited approaches in Systems Engineering (SE) to fulfil such needs, to prevent excessive resource for reaching the agreement on the system concept.

The main objective of this contribution is to investigate how FMECA can get advantages from SE. Many companies have adopted SE as the systematic approach for the design of complex systems (Asbjørnsen, 1992; Haskins, 2008). In fact, SE may help in mediating information exchange among professionals in a simple and concrete way by means of different analyses and models at different detail levels. In this sense, it allows the right person to access the right information at the right time and use it. The adaptation and exploitation of SE approaches and models can assist in maintaining the unified context of the system and ensuring that the interests of different stakeholders are properly understood and considered.

This paper provides a notion through a practical case on to what extent and in which ways the risk analysts think SE methods as effective for supporting FMECA. The following of this paper is organized as follows: Section 2 describes the basis of the subsea gas boosting laboratory that still demands further improvements from a risk perspective. Section 3 discusses the key features of linking and coupling systems engineering and risk analysis models. In Section 4, the proposed model is executed with the practical case and the results are presented in section 5, discussed in section 6 consecutively. Sections 7 presents conclusions.

2 A PRACTICAL CASE

The paper tactically selects an accessible subsea laboratory located at the Department of Mechanical and Industrial Engineering (MTP) at the Norwegian University of Science and Technology (NTNU) to investigate a larger spectrum of risks relevant to subsea gas boosting, as shown in Figure 1. As of today, one challenge for subsea boosting is the compression of wet gas (within

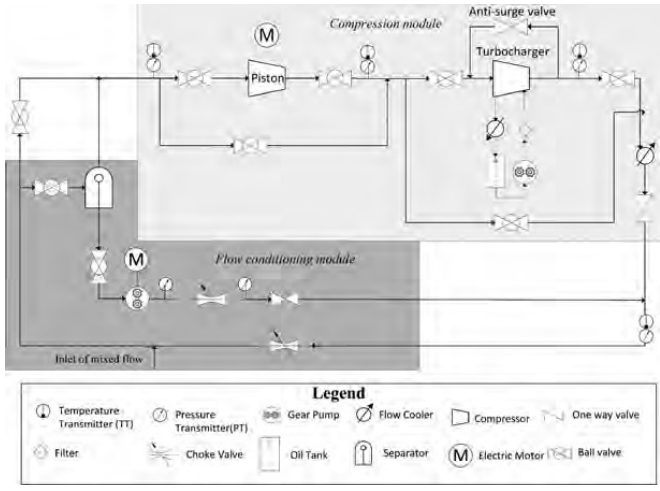


Figure 1. Subsea compression laboratory.

water fraction of 2–20%) since the stratified gas-liquid flow may run the high risk of damaging the traditional compressor. The laboratory is constructed as the pre-testing facility to emulate the different existing solutions for subsea wet gas compression in the Norwegian Continent Shelf, i.e. Ormen Lange and Åsgard (within pre-separation) and Gullfaks (without pre-separation).

This laboratory includes two major modules to test different characteristics of wet gas: the separation module (i.e. the left-bottom) and the compression module (i.e. the right-top). The mixed flow within water fraction (ranged from 0–20%) is emulated by controlling the inlet flow. The implementation of a separation module can separate the water from mixed flow before entering the compression module, and allow studying how the working efficiency and robustness of a separator can influence the whole compression process. The compression module involves a compressor driven by a piston and a compressor driven by the turbocharger, where the piston compressor is very vulnerable by particles and water. Three test scenarios are therefore formulated by the manual close/open of ball valves:

- Wet gas compression with the separation module, where the piston is bypassed
- Wet gas compression without the separation module, where the piston is bypassed
- Dry gas compression, where the piston and turbocharger can compress in the series

The laboratory is almost completed in late 2016, but still demands many improvements in respect to different aspects. This paper exclusively focuses on managing emerged risks of the current structure of the laboratory and devotes to present the obtained results and knowledge for the new development in the industry-size gas boosting system.

3 METHOD

This paper aims to suggest a structured method to enrich the scope of validity of risk assessment by taking advantage from SE. The proposed method propagates SE activities toward risk assessment activities such as FMECA, as shown in Figure 2. SE workshop and FMECA workshop that focus on very different objectives are as the heart of this method. This collaborative method of knowledge transfer enables effective risk management with an objective of dispersing expert knowledge into available tacit knowledge (Alavi & Leidner, 2001).

The starting part of the model is preliminary analysis, which includes defining process goal, defining system along with its boundary, environment and interactions. This facilitates having an overview of the process and to be informed about what is included and what isn't included. SE workshop involves experts (e.g. Designers, operators, managers) to create the static vision of the structure of the system from operational, functional and physical perspectives. SE workshop covers the

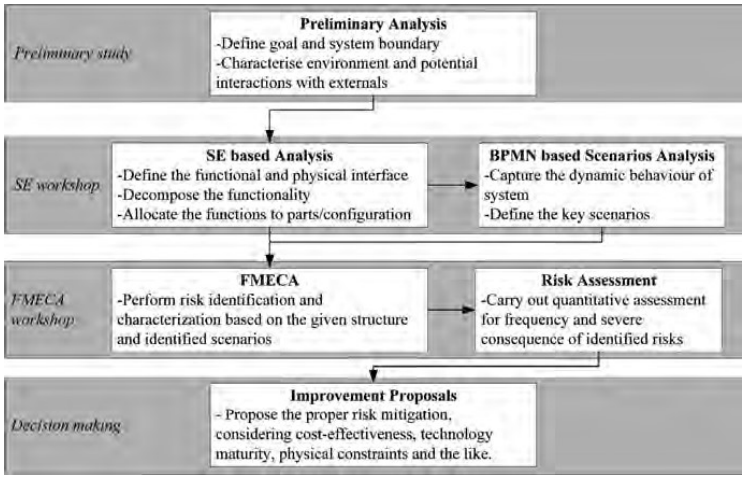


Figure 2. The conceptual map for the proposed method.

interests and the expertise of each contributing stakeholders.SE workshop consists of two concurrent analyses: SE based analysis that covers the operational, functional and physical aspects and the scenario approach that borrows Business Process Model and Notation (BPMN) (White & Miers, 2008). Operational analysis introduces behavior of the system that helps performance based assessment. We can introduce conflict among different component behavior. For example, component C will go off if the component A shuts down or one specific pump may trigger electric supply failure. It solves the conflicts by considering the system function in an ordered sequence of declarations. Functional decomposition specifies how the component functions realize the module functions and how the module functions realize the overall function. Functions that make up another function are grouped together in sets based on ways of achievement. Material, energy and signal flows are viewed as the attributes of these interactions. The functionality is allocated to the preferred parts and layouts. Physical decomposition is made based on the layout of components provided by supplier to show connections between components. This enables us to check interdependency among system components. The availability of the system, including reparable elements can be determined. If one component is out of order, the effect of that on the system or other components can be realized by following the connections. Management personnel can set their work order easily by following the connection.

Designing the scenarios is always an effective way of correctly abstracting the concerns in design. The scenario analysis of a given system is completed on the basis of static vision of its structural decomposition. BPMN can be considered as procedural knowledge representation which represents a set of interconnected procedures (Ligęza & Potempa, 2012). BPMN is therefore considered as a feasible approach to study some scenarios generated from the combination of critical failure, near-miss and even safe states on each interconnected procedure. Both business experts and process experts can easily understand the semantics of BPMN, so this tool is considered feasible to graphically represent the interested scenarios.

The result of SE work is used to conduct FMECA. To carry out the FMECA, multidisciplinary experts are invited to form the team. The team, analyses system components for failure modes. Then potential causes and effects are determined, but forgetting the internal-related or external-related failure modes (DNV-RP-D102, 2012). Involving the scenario-based approach (e.g. BPMN) offers the opportunity to enrich the traditional FMECA. SE workshop combines various discipline knowledge in one common platform and captures multidimensional knowledge into one frame. Different discipline experts analyses the same issue from different angle and may find a different solution (Su & Dou, 2013). It assures universal agreement on a conflicting issue, eliminates bias toward severity rankings, and carry out a detailed analysis of the system structure as well as its process. In addition, generic FMECA contains no dynamic features of the system being analyzed. Using scenario-based analysis as the baseline can assist the risk engineers to clarify the context of each failure modes. The similar approach, called as the scenario-based FMEA was discussed in (Issad, Kloul, & Rauzy, 2017).

After completing FMECA, one can carry out the well-round risk assessment on a basis of FMECA to provide indications for further improvements regarding risk mitigation, recourses and modifications on its structure.

The proposed method is vividly illustrated by the following analysis of the presented case.

4 ANALYSIS

4.1 *Preliminary analysis*

The preliminary analysis defines the preliminary system concept to describe what the system should do, without specifying any functionality and embodies. The analysis covers all the elements that are unmodifiable from engineering perspective, like the external environment of the system, users, legal and regulatory framework and the like. The analysis paves the ground for all the possible technical solutions for the stated problem.

Figure 3 illustrates the operational context within the subsea compressor laboratory, which only indicates what the system do without specifying how to achieve the goal. Different models can be developed on basis of defining operational context of subsea compressor laboratory. For instance, state diagram can be made to check the operational constraints by combining the states of laboratory and those of its external systems, like the energy supply system. The complete preliminary analysis can lay a solid foundation towards the SE workshop that complete the system concept.

4.2 *SE workshop*

The SE workshop executes the analysis stated and discussed above in Section 3, including the functional decomposition and physical decomposition. Functional decomposition is to define the different levels of functionality based on the system mission. Physical decomposition is based on the Process & Instrumentation Diagrams (P&ID) and layout of each component to check physical interactions among subcomponents and allocations. Figure 4 illustrates the physical decomposition of

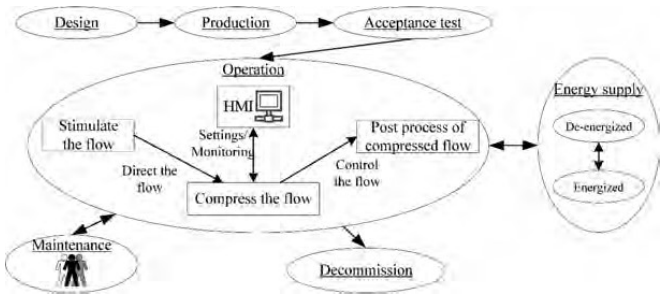


Figure 3. Operational contexts of subsea compressor laboratory.

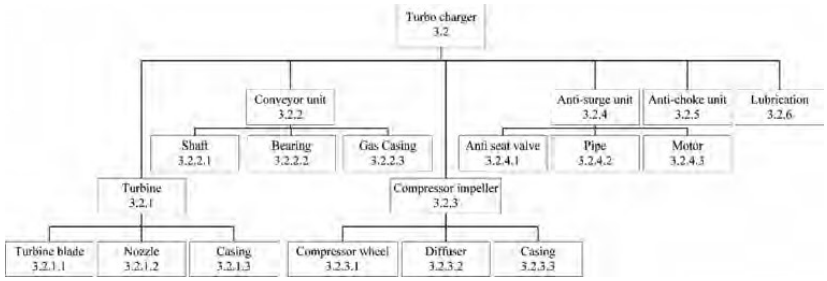


Figure 4. Physical decomposition.

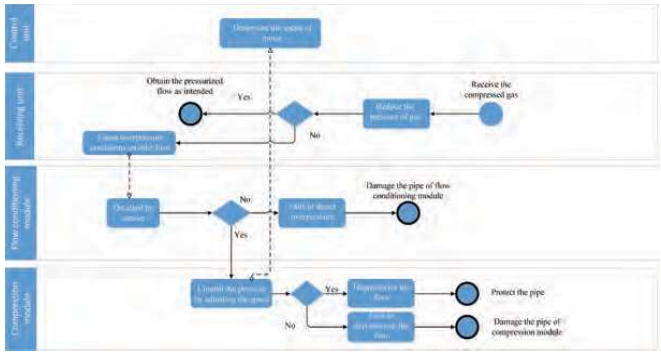


Figure 5. Simplified BPMN for overpressure scenario.

the selected system, the turbo charger to exemplify some key activities in SE workshop.

The decomposition is rather easy to apply for analyzing the functionality and physical structure of the system. One can refine all the operational contexts with sufficient details and trace the changes of functionality and structure through such method. However, this method only describes the system concept statically. Indeed, to complete the well-round risk analysis, we have to carry out the scenario analysis that dynamically describe the events that trigger the transitions between each operational context.

As discussed before, BPMN models are convenient to visualize practical scenarios. Figure 5 presents one selected accident scenario. In Figure 5, the laboratory is tactically divided into

four lanes, including a control unit that is not illustrated in Figure 1. The interfaces (information exchange) between control unit and other lane are indicated by the message flow, i.e. the dashed line. Three decision points are presented to accommodate different missions. The identified operational contexts are also reflected in BPMN model. One can explicitly observe how the control unit influences the whole process of subsea gas compression, and connects each object within distinct activities through BPMN. Here, focus is given to the overall process, system interactions, interface and sequence to work flow, where no time/temporal aspects are considered. Different consequences are specified upon the success of activities, i.e. the availability of corresponding objects. Through generating the accidental scenarios, designers are able to identify the additional needs and carry out complementary analysis to improve the design proposal, see also the summarized result in Section 5.

4.3 *FMECA workshop*

The results from SE workshop are integrated in the FMECA. One advantage is the explicit identification and evaluation of the potential failure modes across physical boundaries. The effect of failure on the subsystems can be studied by analyzing the sequence flow. For instance, the turbocharger compressor receives the flow from the gas intake under the test scenario 2. Once there is a failure or malfunction of the gas intake component, (e.g. Leakage in pipeline or contaminated with liquid from the surroundings), the compressor can be damaged or experience the temporary loss of efficiency. Such risk can be immediately registered when developing FMECA. Another advantage is that BPMN highlights major tasks within the block instead of a corpus of components. In some practices, analysts produce FMECA based on the checklists of physical components (for example Figure 4) as they did not analyze the entirety of the given system concept. By adopting the BPMN model in SE workshop, risk analysts are able to create the FMECA that covers the most significant accident scenarios, which saves a large amount of repetitive and unbalanced works when coordinating the contributions from different design teams.

5 RESULT

Table 1 summarizes some key implications raised after conducting two workshops. The differences between laboratory environment and subsea environment are considered and discussed in the last column of Table 1.

Table 1. Improvement proposal for subsea gas boosting laboratory.

Key issues	Description	Decisions	Relevance for industry-size case
Installation of additional valves, sensors or transmitter	Flow sensor in the water inlet	Must do. The humidity must be controlled to map the characteristics of flow	Not relevant for the flow from the real gas field.
	Pressure sensor in the oil loop	Should do. High pressure may blow the pipe.	Relevant.
	Level transmitter in the oil reservoir	Should do. The implementation can assist in the maintenance (oil refill). Especially when the laboratory is continuously run or stop using for a long time (volatilization of oil)	Highly relevant.
	Flow meter before compressor	Can consider for smooth operation Compressor efficiency decreases with increased mass flow.	Highly relevant.
	Flow mixer	Can consider. The stratified flow runs a higher risk of damaging the compressor than a dispersed homogenous flow.	Not relevant, stratified flows are fairly common even in the real gas field.
	Pressure relief valve in the separator	Should do. The implementation will reduce the risk of separator blow.	The relevance depends on the type and size of separator.

(*Continued*)

Table 1. (*Continued*).

Key issues	Description	Decisions	Relevance for industry-size case
Installation of additional components	Logic control unit connected to all sensors and controllers	Must do, to control the process easily and from a remote location.	Highly relevant.
	Additional filters in the inlet water line	Not necessary if have confidence that supply water is clean	The relevance depends on the needs of removing sands or other particles, requiring expertise from reservoir management.
	A Protective wall around the whole lab	Should do, which will prevent smoke dispersion and reduce fire spread	Highly relevant.
	Protective housing for piston compressor, turbocharger, water pump after the separator	Can consider, as it will prevent from damage in case of water flooding. The cost analysis is needed.	Highly relevant.
Maintenance strategy	Leakage test before the operation	Must do, as it is the most cost-efficient mean to check the integrity of the system.	Only relevant for the site-acceptance test. The leakage sensors are implemented for this purpose.
	Periodic dust cleaning	Must do, as it will reduce the blockage of valves and pipe network.	Not relevant.
	Documentation of operation strategy of system and valves	Must do, as it will reduce human error in operation.	Mostly important.

The results are obtained by considering the major risks within the existing design. One limitation of the current analysis is that the engineering efforts behind each decision are not included. The remaining works are the complementary analysis such as life cycle cost analysis to support the decision-making in the real practice.

6 DISCUSSION

This collaborative model of SE workshop and FMECA workshop makes access to a comprehensive knowledge network of practical experience and expert understanding. This enables identification of potential hazards and implementation of appropriate measures for prevention of accidents. The proposed method enables expert to capture and document the experience they have gained throughout different projects. This can be implemented both in the design phase and in modification phase.

In the traditional approach of FMECA, a failure analysis is mainly carried out on the component level, functional interactions between observed components are not included (Bertsche, 2008). Failure analysis is carried out for the individual process steps. The entire production process is not thoroughly analyzed, for example, the layout of individual component is not considered (Bertsche, 2008). The benefits of developing the FMECA through the identification of key scenarios are listed in the following, based on experiences from practical cases:

- Cross-system effects

It is possible to achieve a holistic and systematic view of the system through SE workshop. The functional analysis assists in comprehending

the effect of failure on subsystem functions and system functions.

- Reasonable and reachable risk reduction measures
Risk reduction measures cover several factors, e.g. maintenance scheduling, decision-making support and barrier management. The architectural analysis can clarify the main constraints that limit in choosing these factors. The coordination between FMECA workshop and SE workshop is therefore concerned with whether the selected structure offers the best balance of these factors.

- More than one single dimension
SE workshop involves experts (e.g. designers, operators, managers) in performing BPMN; operational, functional and physical analysis. This allows to include the interests, expertise and the needs of each stakeholder in the very beginning phase of risk analysis and reflects in the development of FMECA.

In the proposed method, important aspects like interaction between components and environmental effects are considered which gives more confidence in risk analysis and in decision making. An abstruse idea of a system introduces uncertainty in the risk assessment process. The consistent representation of knowledge and system assures that results of risk estimates can be integrated in decision making without less doubt. Only system related uncertainties are being dealt here, which can be mitigated with system knowledge based on experience and expertise.

To present the whole system on like only like P&ID will create a blur on communicating the message. This paper proposes structural breakdown type diagram to represent the physical and functional behavior of the system. The analyses include state in the behavior attribute of a system in the model that describes interdependency and helps performance based assessment.

When the system is complex enough, and one component is serving different functions of the system, it can never be edited as a whole or only through physical or functional dissection. Application of both functional and physical analysis gives a hierarchical breakdown with branches to show connections between components. When one component is out of order, the effect on other components or on the whole system can be observed easily by following the connections, so management personnel can set their work order easily.

If any new component is added to or reduced from the system, editing decomposition diagram is easy which helps to modify FMECA easily. It is often found that in traditional approaches for a change of system, risk assessors have to go through FMECA fully. Prior establishment of physical and functional analysis allows users to modify knowledge easily in case of a change of system.

Effective knowledge transfer and integrated knowledge management help to make a more resilient and reliable system by reducing vulnerability. It helps to develop a better plan for proactive measure to cope with the emergency. These workshops include models for performance and reliability, previous experience, realism of assumptions, representativeness of scenarios along with most critical issues, thoroughness of analysis and first class deliverable.

Effective maintenance also requires integrated information and knowledge system from which maintenance team can get output from other disciplines to make proper maintenance record and work order. Capturing system knowledge effectively facilitates full retrieval of information to implement preventive maintenance on a contrary to corrective maintenance. Failing to do so, increases cost significantly (Motawa & Almarshad, 2013).

Risk engineers often do the risk analysis to compare the risk level to check whether the specified activity is to be complied with the standard. In this prospect, a greater chance for improvement remains out of scope and behind the paperwork. By the arrangement of thinking around systematic activities described earlier, risk can be communicated effectively and efficiently. The quality of risk assessment can be improved by capturing and identification of all possible issues systematically. By sharing with one another's information, it is possible to get a better risk picture in more than one single dimension (Su & Dou, 2013).

However, going through all details is time consuming as there remains a lot of overlaps and repetitions among functions. It is difficult to define the scope of subsystem when one single component performs two functions. It is also questionable whether to assume the previous work as reliable enough or not. Finding necessary expert and shareholders' opinion on a timely manner need proper planning. The execution of the proposed method needs a high management capability of the organization. An organization should have a commitment to provide resources, freedom and time needed to acquire information. Implementing the analysis in development phase makes it possible to identify weak spots and comparative tests can be carried out.

7 CONCLUSION

Modern society deals with a larger spectrum of risk and a larger spectrum of stakeholders, of interest, value and knowledge. Recognizing the wider scope of risk leads to a positive evolution in managing risk. A structured communication model can help in this respect. In this paper, we

presented how SE may help in capturing different nodes of a system for effective risk evaluation, through the basic analysis technique like FMECA. The proposed method is checked with a subsea gas boosting laboratory where the case study assures more confidence in making development proposal and risk mitigation. By doing this type of analyses in the development phase, it is possible to identify weak spots and comparative tests can be carried out. Modifications in the design phase saves cost and preventive measures can be taken.

As a future improvement, a consequence study can be included in detail and should be checked with other applications. The paper also suggests AltaRica 3.0 to encode the FMECA for quantitative risk assessment. This recent achievement has been brought to the forefront in the risk analysis community, see also more details about this modelling language in (Prosvirnova, 2014). This modelling formalism suggests taking the advantages from a structuring paradigm, i.e. S2ML (Batteux, Prosvirnova, & Rauzy, 2015), and a sufficient mathematical framework, i.e. GTS (Rauzy, 2008). With the support of this modelling language, the analysts can provide indications of the system structure as well as the operational process.

ACKNOWLEDGEMENTS

The authors would gratefully thank Christian Holden, for kindly sharing his knowledge and design experience about the subsea laboratory at the Department of Mechanical and Industrial Engineering at the Norwegian University of Science and Technology (NTNU) and for patiently answering technical questions.

REFERENCES

Alavi, M., & Leidner, D.E. (2001). Review: Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*, 107–136.

Asbjørnsen, O. (1992). *Systems engineering principles and practices*. Maryland, USA: Skarpodd.

Batteux, M., Prosvirnova, T., & Rauzy, A. (2015). *System Structure Modeling Language (S2ML)*.

Bertsche, B. (2008). *Reliability in automotive and mechanical engineering: determination of component and system reliability*: Springer Science & Business Media.

DNV-RP-D102. (2012). *Failure Mode and Effect Analysis (FMEA) of Redundant Systems*. Høvik, Norway: DNV.

Haskins, C. (2008). *Systems engineering analyzed, synthesized, and applied to sustainable industrial park development*. PhD thesis: NTNU.

ISO 31000. (2009). *Risk management-Priciples and guidelines*: International Organization for Standardization.

Issad, M., Kloul, L., & Rauzy, A. (2017). *A scenario-based FMEA method and its evaluation in a railway context*. Paper presented at the Reliability and Maintainability Symposium (RAMS).

Kirsch, P., Hineb, A., & Maybury, T. (2015). A model for the implementation of industry-wide knowledge sharing to improve risk management practice. *Safety Science, 80*, 66–76.

Ligęza, A., & Potempa, T. (2012). *Artificial intelligence for knowledge management with bpmn and rules*. Paper presented at the IFIP International Workshop on Artificial Intelligence for Knowledge Management.

Motawa, I., & Almarshad, A. (2013). A knowledge-based BIM system for building maintenance. *Automation in Construction, 29*, 173–182.

NORSOK Z-013. (2010). *Risk and emergency preparedness assessment*.

Prosvirnova, T. (2014). *AltaRica 3.0: a Model-Based approach for Safety Analyses*. Computational Engineering, Finance, and Science [cs.CE] Ecole Polytechnique.

Rauzy, A. (2008). Guarded transition systems: A new states/events formalism for reliability studies. *Proceedings of the Institution of Mechanical Engineers. Part O, Journal of risk and reliability, 222*(4).

Rice, R.G., & Spence, P.R. (2016). Thor visits Lexington: Exploration of the knowledge-sharing gap and risk management learning in social media during multiple winter storms. *Computers in Human Behavior, 65*(612–618).

Su, E., & Dou, J. (2013). How Does Knowledge Sharing Among Advisors From Different Disciplines Affect the Quality of the Services Provided to the Family Business Client? An Investigation From the Family Business Advisor's Perspective. *Family Business Review, 26*(3), 256–270. doi:10.1177/0894486513491978.

White, S.A., & Miers, D. (2008). *BPMN Modelling and Reference Guide: Understanding and Using BPMN*. usa: Future Strategies.

Previous PhD theses published at the Department of Marine Technology
(earlier: Faculty of Marine Technology)
NORWEGIAN UNIVERSITY OF SCIENCE AND TECHNOLOGY

Report No.	Author	Title
	Kavlie, Dag	Optimization of Plane Elastic Grillages, 1967
	Hansen, Hans R.	Man-Machine Communication and Data-Storage Methods in Ship Structural Design, 1971
	Gisvold, Kaare M.	A Method for non-linear mixed -integer programming and its Application to Design Problems, 1971
	Lund, Sverre	Tanker Frame Optimalization by means of SUMT-Transformation and Behaviour Models, 1971
	Vinje, Tor	On Vibration of Spherical Shells Interacting with Fluid, 1972
	Lorentz, Jan D.	Tank Arrangement for Crude Oil Carriers in Accordance with the new Anti-Pollution Regulations, 1975
	Carlsen, Carl A.	Computer-Aided Design of Tanker Structures, 1975
	Larsen, Carl M.	Static and Dynamic Analysis of Offshore Pipelines during Installation, 1976
UR-79-01	Brigt Hatlestad, MK	The finite element method used in a fatigue evaluation of fixed offshore platforms. (Dr.Ing. Thesis)
UR-79-02	Erik Pettersen, MK	Analysis and design of cellular structures. (Dr.Ing. Thesis)
UR-79-03	Sverre Valsgård, MK	Finite difference and finite element methods applied to nonlinear analysis of plated structures. (Dr.Ing. Thesis)
UR-79-04	Nils T. Nordsve, MK	Finite element collapse analysis of structural members considering imperfections and stresses due to fabrication. (Dr.Ing. Thesis)
UR-79-05	Ivar J. Fylling, MK	Analysis of towline forces in ocean towing systems. (Dr.Ing. Thesis)
UR-80-06	Nils Sandsmark, MM	Analysis of Stationary and Transient Heat Conduction by the Use of the Finite Element Method. (Dr.Ing. Thesis)
UR-80-09	Sverre Haver, MK	Analysis of uncertainties related to the stochastic modeling of ocean waves. (Dr.Ing. Thesis)
UR-81-15	Odland, Jonas	On the Strength of welded Ring stiffened cylindrical Shells primarily subjected to axial Compression
UR-82-17	Engesvik, Knut	Analysis of Uncertainties in the fatigue Capacity of Welded Joints
UR-82-18	Rye, Henrik	Ocean wave groups

UR-83-30	Eide, Oddvar Inge	On Cumulative Fatigue Damage in Steel Welded Joints
UR-83-33	Mo, Olav	Stochastic Time Domain Analysis of Slender Offshore Structures
UR-83-34	Amdahl, Jørgen	Energy absorption in Ship-platform impacts
UR-84-37	Mørch, Morten	Motions and mooring forces of semi submersibles as determined by full-scale measurements and theoretical analysis
UR-84-38	Soares, C. Guedes	Probabilistic models for load effects in ship structures
UR-84-39	Aarsnes, Jan V.	Current forces on ships
UR-84-40	Czujko, Jerzy	Collapse Analysis of Plates subjected to Biaxial Compression and Lateral Load
UR-85-46	Alf G. Engseth, MK	Finite element collapse analysis of tubular steel offshore structures. (Dr.Ing. Thesis)
UR-86-47	Dengody Sheshappa, MP	A Computer Design Model for Optimizing Fishing Vessel Designs Based on Techno-Economic Analysis. (Dr.Ing. Thesis)
UR-86-48	Vidar Aanesland, MH	A Theoretical and Numerical Study of Ship Wave Resistance. (Dr.Ing. Thesis)
UR-86-49	Heinz-Joachim Wessel, MK	Fracture Mechanics Analysis of Crack Growth in Plate Girders. (Dr.Ing. Thesis)
UR-86-50	Jon Taby, MK	Ultimate and Post-ultimate Strength of Dented Tubular Members. (Dr.Ing. Thesis)
UR-86-51	Walter Lian, MH	A Numerical Study of Two-Dimensional Separated Flow Past Bluff Bodies at Moderate KC-Numbers. (Dr.Ing. Thesis)
UR-86-52	Bjørn Sortland, MH	Force Measurements in Oscillating Flow on Ship Sections and Circular Cylinders in a U-Tube Water Tank. (Dr.Ing. Thesis)
UR-86-53	Kurt Strand, MM	A System Dynamic Approach to One-dimensional Fluid Flow. (Dr.Ing. Thesis)
UR-86-54	Arne Edvin Løken, MH	Three Dimensional Second Order Hydrodynamic Effects on Ocean Structures in Waves. (Dr.Ing. Thesis)
UR-86-55	Sigurd Falch, MH	A Numerical Study of Slamming of Two-Dimensional Bodies. (Dr.Ing. Thesis)
UR-87-56	Arne Braathen, MH	Application of a Vortex Tracking Method to the Prediction of Roll Damping of a Two-Dimension Floating Body. (Dr.Ing. Thesis)
UR-87-57	Bernt Leira, MK	Gaussian Vector Processes for Reliability Analysis involving Wave-Induced Load Effects. (Dr.Ing. Thesis)

UR-87-58	Magnus Småvik, MM	Thermal Load and Process Characteristics in a Two-Stroke Diesel Engine with Thermal Barriers (in Norwegian). (Dr.Ing. Thesis)
MTA-88-59	Bernt Arild Bremdal, MP	An Investigation of Marine Installation Processes – A Knowledge - Based Planning Approach. (Dr.Ing. Thesis)
MTA-88-60	Xu Jun, MK	Non-linear Dynamic Analysis of Space-framed Offshore Structures. (Dr.Ing. Thesis)
MTA-89-61	Gang Miao, MH	Hydrodynamic Forces and Dynamic Responses of Circular Cylinders in Wave Zones. (Dr.Ing. Thesis)
MTA-89-62	Martin Greenhow, MH	Linear and Non-Linear Studies of Waves and Floating Bodies. Part I and Part II. (Dr.Techn. Thesis)
MTA-89-63	Chang Li, MH	Force Coefficients of Spheres and Cubes in Oscillatory Flow with and without Current. (Dr.Ing. Thesis
MTA-89-64	Hu Ying, MP	A Study of Marketing and Design in Development of Marine Transport Systems. (Dr.Ing. Thesis)
MTA-89-65	Arild Jæger, MH	Seakeeping, Dynamic Stability and Performance of a Wedge Shaped Planing Hull. (Dr.Ing. Thesis)
MTA-89-66	Chan Siu Hung, MM	The dynamic characteristics of tilting-pad bearings
MTA-89-67	Kim Wikstrøm, MP	Analysis av projekteringen for ett offshore projekt. (Licenciat-avhandling)
MTA-89-68	Jiao Guoyang, MK	Reliability Analysis of Crack Growth under Random Loading, considering Model Updating. (Dr.Ing. Thesis)
MTA-89-69	Arnt Olufsen, MK	Uncertainty and Reliability Analysis of Fixed Offshore Structures. (Dr.Ing. Thesis)
MTA-89-70	Wu Yu-Lin, MR	System Reliability Analyses of Offshore Structures using improved Truss and Beam Models. (Dr.Ing. Thesis)
MTA-90-71	Jan Roger Hoff, MH	Three-dimensional Green function of a vessel with forward speed in waves. (Dr.Ing. Thesis)
MTA-90-72	Rong Zhao, MH	Slow-Drift Motions of a Moored Two-Dimensional Body in Irregular Waves. (Dr.Ing. Thesis)
MTA-90-73	Atle Minsaas, MP	Economical Risk Analysis. (Dr.Ing. Thesis)
MTA-90-74	Knut-Aril Farnes, MK	Long-term Statistics of Response in Non-linear Marine Structures. (Dr.Ing. Thesis)
MTA-90-75	Torbjørn Sotberg, MK	Application of Reliability Methods for Safety Assessment of Submarine Pipelines. (Dr.Ing. Thesis)
MTA-90-76	Zeuthen, Steffen, MP	SEAMAID. A computational model of the design process in a constraint-based logic programming environment. An example from the offshore

		domain. (Dr.Ing. Thesis)
MTA-91-77	Haagensen, Sven, MM	Fuel Dependant Cyclic Variability in a Spark Ignition Engine - An Optical Approach. (Dr.Ing. Thesis)
MTA-91-78	Løland, Geir, MH	Current forces on and flow through fish farms. (Dr.Ing. Thesis)
MTA-91-79	Hoen, Christopher, MK	System Identification of Structures Excited by Stochastic Load Processes. (Dr.Ing. Thesis)
MTA-91-80	Haugen, Stein, MK	Probabilistic Evaluation of Frequency of Collision between Ships and Offshore Platforms. (Dr.Ing. Thesis)
MTA-91-81	Sødahl, Nils, MK	Methods for Design and Analysis of Flexible Risers. (Dr.Ing. Thesis)
MTA-91-82	Ormberg, Harald, MK	Non-linear Response Analysis of Floating Fish Farm Systems. (Dr.Ing. Thesis)
MTA-91-83	Marley, Mark J., MK	Time Variant Reliability under Fatigue Degradation. (Dr.Ing. Thesis)
MTA-91-84	Krokstad, Jørgen R., MH	Second-order Loads in Multidirectional Seas. (Dr.Ing. Thesis)
MTA-91-85	Molteberg, Gunnar A., MM	The Application of System Identification Techniques to Performance Monitoring of Four Stroke Turbocharged Diesel Engines. (Dr.Ing. Thesis)
MTA-92-86	Mørch, Hans Jørgen Bjelke, MH	Aspects of Hydrofoil Design: with Emphasis on Hydrofoil Interaction in Calm Water. (Dr.Ing. Thesis)
MTA-92-87	Chan Siu Hung, MM	Nonlinear Analysis of Rotordynamic Instabilities in Highspeed Turbomachinery. (Dr.Ing. Thesis)
MTA-92-88	Bessason, Bjarni, MK	Assessment of Earthquake Loading and Response of Seismically Isolated Bridges. (Dr.Ing. Thesis)
MTA-92-89	Langli, Geir, MP	Improving Operational Safety through exploitation of Design Knowledge - an investigation of offshore platform safety. (Dr.Ing. Thesis)
MTA-92-90	Sævik, Svein, MK	On Stresses and Fatigue in Flexible Pipes. (Dr.Ing. Thesis)
MTA-92-91	Ask, Tor Ø., MM	Ignition and Flame Growth in Lean Gas-Air Mixtures. An Experimental Study with a Schlieren System. (Dr.Ing. Thesis)
MTA-86-92	Hessen, Gunnar, MK	Fracture Mechanics Analysis of Stiffened Tubular Members. (Dr.Ing. Thesis)
MTA-93-93	Steinebach, Christian, MM	Knowledge Based Systems for Diagnosis of Rotating Machinery. (Dr.Ing. Thesis)
MTA-93-94	Dalane, Jan Inge, MK	System Reliability in Design and Maintenance of

		Fixed Offshore Structures. (Dr.Ing. Thesis)
MTA-93-95	Steen, Sverre, MH	Cobblestone Effect on SES. (Dr.Ing. Thesis)
MTA-93-96	Karunakaran, Daniel, MK	Nonlinear Dynamic Response and Reliability Analysis of Drag-dominated Offshore Platforms. (Dr.Ing. Thesis)
MTA-93-97	Hagen, Arnulf, MP	The Framework of a Design Process Language. (Dr.Ing. Thesis)
MTA-93-98	Nordrik, Rune, MM	Investigation of Spark Ignition and Autoignition in Methane and Air Using Computational Fluid Dynamics and Chemical Reaction Kinetics. A Numerical Study of Ignition Processes in Internal Combustion Engines. (Dr.Ing. Thesis)
MTA-94-99	Passano, Elizabeth, MK	Efficient Analysis of Nonlinear Slender Marine Structures. (Dr.Ing. Thesis)
MTA-94-100	Kvålsvold, Jan, MH	Hydroelastic Modelling of Wetdeck Slamming on Multihull Vessels. (Dr.Ing. Thesis)
MTA-94-102	Bech, Sidsel M., MK	Experimental and Numerical Determination of Stiffness and Strength of GRP/PVC Sandwich Structures. (Dr.Ing. Thesis)
MTA-95-103	Paulsen, Hallvard, MM	A Study of Transient Jet and Spray using a Schlieren Method and Digital Image Processing. (Dr.Ing. Thesis)
MTA-95-104	Hovde, Geir Olav, MK	Fatigue and Overload Reliability of Offshore Structural Systems, Considering the Effect of Inspection and Repair. (Dr.Ing. Thesis)
MTA-95-105	Wang, Xiaozhi, MK	Reliability Analysis of Production Ships with Emphasis on Load Combination and Ultimate Strength. (Dr.Ing. Thesis)
MTA-95-106	Ulstein, Tore, MH	Nonlinear Effects of a Flexible Stern Seal Bag on Cobblestone Oscillations of an SES. (Dr.Ing. Thesis)
MTA-95-107	Solaas, Frøydis, MH	Analytical and Numerical Studies of Sloshing in Tanks. (Dr.Ing. Thesis)
MTA-95-108	Hellan, Øyvind, MK	Nonlinear Pushover and Cyclic Analyses in Ultimate Limit State Design and Reassessment of Tubular Steel Offshore Structures. (Dr.Ing. Thesis)
MTA-95-109	Hermundstad, Ole A., MK	Theoretical and Experimental Hydroelastic Analysis of High Speed Vessels. (Dr.Ing. Thesis)
MTA-96-110	Bratland, Anne K., MH	Wave-Current Interaction Effects on Large-Volume Bodies in Water of Finite Depth. (Dr.Ing. Thesis)
MTA-96-111	Herfjord, Kjell, MH	A Study of Two-dimensional Separated Flow by a Combination of the Finite Element Method and Navier-Stokes Equations. (Dr.Ing. Thesis)
MTA-96-112	Æsøy, Vilmar, MM	Hot Surface Assisted Compression Ignition in a Direct Injection Natural Gas Engine. (Dr.Ing.

		Thesis)
MTA-96-113	Eknes, Monika L., MK	Escalation Scenarios Initiated by Gas Explosions on Offshore Installations. (Dr.Ing. Thesis)
MTA-96-114	Erikstad, Stein O., MP	A Decision Support Model for Preliminary Ship Design. (Dr.Ing. Thesis)
MTA-96-115	Pedersen, Egil, MH	A Nautical Study of Towed Marine Seismic Streamer Cable Configurations. (Dr.Ing. Thesis)
MTA-97-116	Moksnes, Paul O., MM	Modelling Two-Phase Thermo-Fluid Systems Using Bond Graphs. (Dr.Ing. Thesis)
MTA-97-117	Halse, Karl H., MK	On Vortex Shedding and Prediction of Vortex-Induced Vibrations of Circular Cylinders. (Dr.Ing. Thesis)
MTA-97-118	Igland, Ragnar T., MK	Reliability Analysis of Pipelines during Laying, considering Ultimate Strength under Combined Loads. (Dr.Ing. Thesis)
MTA-97-119	Pedersen, Hans-P., MP	Levendefiskteknologi for fiskefartøy. (Dr.Ing. Thesis)
MTA-98-120	Vikestad, Kyrre, MK	Multi-Frequency Response of a Cylinder Subjected to Vortex Shedding and Support Motions. (Dr.Ing. Thesis)
MTA-98-121	Azadi, Mohammad R. E., MK	Analysis of Static and Dynamic Pile-Soil-Jacket Behaviour. (Dr.Ing. Thesis)
MTA-98-122	Ulltang, Terje, MP	A Communication Model for Product Information. (Dr.Ing. Thesis)
MTA-98-123	Torbergsen, Erik, MM	Impeller/Diffuser Interaction Forces in Centrifugal Pumps. (Dr.Ing. Thesis)
MTA-98-124	Hansen, Edmond, MH	A Discrete Element Model to Study Marginal Ice Zone Dynamics and the Behaviour of Vessels Moored in Broken Ice. (Dr.Ing. Thesis)
MTA-98-125	Videiro, Paulo M., MK	Reliability Based Design of Marine Structures. (Dr.Ing. Thesis)
MTA-99-126	Mainçon, Philippe, MK	Fatigue Reliability of Long Welds Application to Titanium Risers. (Dr.Ing. Thesis)
MTA-99-127	Haugen, Elin M., MH	Hydroelastic Analysis of Slamming on Stiffened Plates with Application to Catamaran Wetdecks. (Dr.Ing. Thesis)
MTA-99-128	Langhelle, Nina K., MK	Experimental Validation and Calibration of Nonlinear Finite Element Models for Use in Design of Aluminium Structures Exposed to Fire. (Dr.Ing. Thesis)
MTA-99-129	Berstad, Are J., MK	Calculation of Fatigue Damage in Ship Structures. (Dr.Ing. Thesis)
MTA-99-130	Andersen, Trond M., MM	Short Term Maintenance Planning. (Dr.Ing. Thesis)

MTA-99-131	Tveiten, Bård Wathne, MK	Fatigue Assessment of Welded Aluminium Ship Details. (Dr.Ing. Thesis)
MTA-99-132	Søreide, Fredrik, MP	Applications of underwater technology in deep water archaeology. Principles and practice. (Dr.Ing. Thesis)
MTA-99-133	Tønnessen, Rune, MH	A Finite Element Method Applied to Unsteady Viscous Flow Around 2D Blunt Bodies With Sharp Corners. (Dr.Ing. Thesis)
MTA-99-134	Elvekrok, Dag R., MP	Engineering Integration in Field Development Projects in the Norwegian Oil and Gas Industry. The Supplier Management of Norne. (Dr.Ing. Thesis)
MTA-99-135	Fagerholt, Kjetil, MP	Optimeringsbaserte Metoder for Ruteplanlegging innen skipsfart. (Dr.Ing. Thesis)
MTA-99-136	Bysveen, Marie, MM	Visualization in Two Directions on a Dynamic Combustion Rig for Studies of Fuel Quality. (Dr.Ing. Thesis)
MTA-2000-137	Storteig, Eskild, MM	Dynamic characteristics and leakage performance of liquid annular seals in centrifugal pumps. (Dr.Ing. Thesis)
MTA-2000-138	Sagli, Gro, MK	Model uncertainty and simplified estimates of long term extremes of hull girder loads in ships. (Dr.Ing. Thesis)
MTA-2000-139	Tronstad, Harald, MK	Nonlinear analysis and design of cable net structures like fishing gear based on the finite element method. (Dr.Ing. Thesis)
MTA-2000-140	Kroneberg, André, MP	Innovation in shipping by using scenarios. (Dr.Ing. Thesis)
MTA-2000-141	Haslum, Herbjørn Alf, MH	Simplified methods applied to nonlinear motion of spar platforms. (Dr.Ing. Thesis)
MTA-2001-142	Samdal, Ole Johan, MM	Modelling of Degradation Mechanisms and Stressor Interaction on Static Mechanical Equipment Residual Lifetime. (Dr.Ing. Thesis)
MTA-2001-143	Baarholm, Rolf Jarle, MH	Theoretical and experimental studies of wave impact underneath decks of offshore platforms. (Dr.Ing. Thesis)
MTA-2001-144	Wang, Lihua, MK	Probabilistic Analysis of Nonlinear Wave-induced Loads on Ships. (Dr.Ing. Thesis)
MTA-2001-145	Kristensen, Odd H. Holt, MK	Ultimate Capacity of Aluminium Plates under Multiple Loads, Considering HAZ Properties. (Dr.Ing. Thesis)
MTA-2001-146	Greco, Marilena, MH	A Two-Dimensional Study of Green-Water Loading. (Dr.Ing. Thesis)
MTA-2001-147	Heggelund, Svein E., MK	Calculation of Global Design Loads and Load Effects in Large High Speed Catamarans. (Dr.Ing. Thesis)

MTA-2001-148	Babalola, Olusegun T., MK	Fatigue Strength of Titanium Risers – Defect Sensitivity. (Dr.Ing. Thesis)
MTA-2001-149	Mohammed, Abuu K., MK	Nonlinear Shell Finite Elements for Ultimate Strength and Collapse Analysis of Ship Structures. (Dr.Ing. Thesis)
MTA-2002-150	Holmedal, Lars E., MH	Wave-current interactions in the vicinity of the sea bed. (Dr.Ing. Thesis)
MTA-2002-151	Rognebakke, Olav F., MH	Sloshing in rectangular tanks and interaction with ship motions. (Dr.Ing. Thesis)
MTA-2002-152	Lader, Pål Furset, MH	Geometry and Kinematics of Breaking Waves. (Dr.Ing. Thesis)
MTA-2002-153	Yang, Qinzheng, MH	Wash and wave resistance of ships in finite water depth. (Dr.Ing. Thesis)
MTA-2002-154	Melhus, Øyvin, MM	Utilization of VOC in Diesel Engines. Ignition and combustion of VOC released by crude oil tankers. (Dr.Ing. Thesis)
MTA-2002-155	Ronæss, Marit, MH	Wave Induced Motions of Two Ships Advancing on Parallel Course. (Dr.Ing. Thesis)
MTA-2002-156	Økland, Ole D., MK	Numerical and experimental investigation of whipping in twin hull vessels exposed to severe wet deck slamming. (Dr.Ing. Thesis)
MTA-2002-157	Ge, Chunhua, MK	Global Hydroelastic Response of Catamarans due to Wet Deck Slamming. (Dr.Ing. Thesis)
MTA-2002-158	Byklum, Eirik, MK	Nonlinear Shell Finite Elements for Ultimate Strength and Collapse Analysis of Ship Structures. (Dr.Ing. Thesis)
IMT-2003-1	Chen, Haibo, MK	Probabilistic Evaluation of FPSO-Tanker Collision in Tandem Offloading Operation. (Dr.Ing. Thesis)
IMT-2003-2	Skaugset, Kjetil Bjørn, MK	On the Suppression of Vortex Induced Vibrations of Circular Cylinders by Radial Water Jets. (Dr.Ing. Thesis)
IMT-2003-3	Chezhian, Muthu	Three-Dimensional Analysis of Slamming. (Dr.Ing. Thesis)
IMT-2003-4	Buhaug, Øyvind	Deposit Formation on Cylinder Liner Surfaces in Medium Speed Engines. (Dr.Ing. Thesis)
IMT-2003-5	Tregde, Vidar	Aspects of Ship Design: Optimization of Aft Hull with Inverse Geometry Design. (Dr.Ing. Thesis)
IMT-2003-6	Wist, Hanne Therese	Statistical Properties of Successive Ocean Wave Parameters. (Dr.Ing. Thesis)
IMT-2004-7	Ransau, Samuel	Numerical Methods for Flows with Evolving Interfaces. (Dr.Ing. Thesis)
IMT-	Soma, Torkel	Blue-Chip or Sub-Standard. A data interrogation

2004-8		approach of identity safety characteristics of shipping organization. (Dr.Ing. Thesis)
IMT-2004-9	Ersdal, Svein	An experimental study of hydrodynamic forces on cylinders and cables in near axial flow. (Dr.Ing. Thesis)
IMT-2005-10	Brodtkorb, Per Andreas	The Probability of Occurrence of Dangerous Wave Situations at Sea. (Dr.Ing. Thesis)
IMT-2005-11	Yttervik, Rune	Ocean current variability in relation to offshore engineering. (Dr.Ing. Thesis)
IMT-2005-12	Fredheim, Arne	Current Forces on Net-Structures. (Dr.Ing. Thesis)
IMT-2005-13	Heggernes, Kjetil	Flow around marine structures. (Dr.Ing. Thesis
IMT-2005-14	Fouques, Sebastien	Lagrangian Modelling of Ocean Surface Waves and Synthetic Aperture Radar Wave Measurements. (Dr.Ing. Thesis)
IMT-2006-15	Holm, Håvard	Numerical calculation of viscous free surface flow around marine structures. (Dr.Ing. Thesis)
IMT-2006-16	Bjørheim, Lars G.	Failure Assessment of Long Through Thickness Fatigue Cracks in Ship Hulls. (Dr.Ing. Thesis)
IMT-2006-17	Hansson, Lisbeth	Safety Management for Prevention of Occupational Accidents. (Dr.Ing. Thesis)
IMT-2006-18	Zhu, Xinying	Application of the CIP Method to Strongly Nonlinear Wave-Body Interaction Problems. (Dr.Ing. Thesis)
IMT-2006-19	Reite, Karl Johan	Modelling and Control of Trawl Systems. (Dr.Ing. Thesis)
IMT-2006-20	Smogeli, Øyvind Notland	Control of Marine Propellers. From Normal to Extreme Conditions. (Dr.Ing. Thesis)
IMT-2007-21	Storhaug, Gaute	Experimental Investigation of Wave Induced Vibrations and Their Effect on the Fatigue Loading of Ships. (Dr.Ing. Thesis)
IMT-2007-22	Sun, Hui	A Boundary Element Method Applied to Strongly Nonlinear Wave-Body Interaction Problems. (PhD Thesis, CeSOS)
IMT-2007-23	Rustad, Anne Marthine	Modelling and Control of Top Tensioned Risers. (PhD Thesis, CeSOS)
IMT-2007-24	Johansen, Vegar	Modelling flexible slender system for real-time simulations and control applications
IMT-2007-25	Wroldsen, Anders Sunde	Modelling and control of tensegrity structures. (PhD Thesis, CeSOS)
IMT-2007-26	Aronsen, Kristoffer Høye	An experimental investigation of in-line and combined inline and cross flow vortex induced vibrations. (Dr. avhandling, IMT)
IMT-	Gao, Zhen	Stochastic Response Analysis of Mooring Systems

2007-27		with Emphasis on Frequency-domain Analysis of Fatigue due to Wide-band Response Processes (PhD Thesis, CeSOS)
IMT-2007-28	Thorstensen, Tom Anders	Lifetime Profit Modelling of Ageing Systems Utilizing Information about Technical Condition. (Dr.ing. thesis, IMT)
IMT-2008-29	Refsnes, Jon Erling Gorset	Nonlinear Model-Based Control of Slender Body AUVs (PhD Thesis, IMT)
IMT-2008-30	Berntsen, Per Ivar B.	Structural Reliability Based Position Mooring. (PhD-Thesis, IMT)
IMT-2008-31	Ye, Naiquan	Fatigue Assessment of Aluminium Welded Box-stiffener Joints in Ships (Dr.ing. thesis, IMT)
IMT-2008-32	Radan, Damir	Integrated Control of Marine Electrical Power Systems. (PhD-Thesis, IMT)
IMT-2008-33	Thomassen, Paul	Methods for Dynamic Response Analysis and Fatigue Life Estimation of Floating Fish Cages. (Dr.ing. thesis, IMT)
IMT-2008-34	Pákozdi, Csaba	A Smoothed Particle Hydrodynamics Study of Two-dimensional Nonlinear Sloshing in Rectangular Tanks. (Dr.ing.thesis, IMT/ CeSOS)
IMT-2007-35	Grytøyr, Guttorm	A Higher-Order Boundary Element Method and Applications to Marine Hydrodynamics. (Dr.ing.thesis, IMT)
IMT-2008-36	Drummen, Ingo	Experimental and Numerical Investigation of Nonlinear Wave-Induced Load Effects in Containerships considering Hydroelasticity. (PhD thesis, CeSOS)
IMT-2008-37	Skejic, Renato	Maneuvering and Seakeeping of a Singel Ship and of Two Ships in Interaction. (PhD-Thesis, CeSOS)
IMT-2008-38	Harlem, Alf	An Age-Based Replacement Model for Repairable Systems with Attention to High-Speed Marine Diesel Engines. (PhD-Thesis, IMT)
IMT-2008-39	Alsos, Hagbart S.	Ship Grounding. Analysis of Ductile Fracture, Bottom Damage and Hull Girder Response. (PhD-thesis, IMT)
IMT-2008-40	Graczyk, Mateusz	Experimental Investigation of Sloshing Loading and Load Effects in Membrane LNG Tanks Subjected to Random Excitation. (PhD-thesis, CeSOS)
IMT-2008-41	Taghipour, Reza	Efficient Prediction of Dynamic Response for Flexible amd Multi-body Marine Structures. (PhD-thesis, CeSOS)
IMT-2008-42	Ruth, Eivind	Propulsion control and thrust allocation on marine vessels. (PhD thesis, CeSOS)
IMT-2008-43	Nystad, Bent Helge	Technical Condition Indexes and Remaining Useful Life of Aggregated Systems. PhD thesis, IMT

IMT-2008-44	Soni, Prashant Kumar	Hydrodynamic Coefficients for Vortex Induced Vibrations of Flexible Beams, PhD thesis, CeSOS
IMT-2009-45	Amlashi, Hadi K.K.	Ultimate Strength and Reliability-based Design of Ship Hulls with Emphasis on Combined Global and Local Loads. PhD Thesis, IMT
IMT-2009-46	Pedersen, Tom Arne	Bond Graph Modelling of Marine Power Systems. PhD Thesis, IMT
IMT-2009-47	Kristiansen, Trygve	Two-Dimensional Numerical and Experimental Studies of Piston-Mode Resonance. PhD-Thesis, CeSOS
IMT-2009-48	Ong, Muk Chen	Applications of a Standard High Reynolds Number Model and a Stochastic Scour Prediction Model for Marine Structures. PhD-thesis, IMT
IMT-2009-49	Hong, Lin	Simplified Analysis and Design of Ships subjected to Collision and Grounding. PhD-thesis, IMT
IMT-2009-50	Koushan, Kamran	Vortex Induced Vibrations of Free Span Pipelines, PhD thesis, IMT
IMT-2009-51	Korsvik, Jarl Eirik	Heuristic Methods for Ship Routing and Scheduling. PhD-thesis, IMT
IMT-2009-52	Lee, Jihoon	Experimental Investigation and Numerical in Analyzing the Ocean Current Displacement of Longlines. Ph.d.-Thesis, IMT.
IMT-2009-53	Vestbøstad, Tone Gran	A Numerical Study of Wave-in-Deck Impact usin a Two-Dimensional Constrained Interpolation Profile Method, Ph.d.thesis, CeSOS.
IMT-2009-54	Bruun, Kristine	Bond Graph Modelling of Fuel Cells for Marine Power Plants. Ph.d.-thesis, IMT
IMT 2009-55	Holstad, Anders	Numerical Investigation of Turbulence in a Sekwed Three-Dimensional Channel Flow, Ph.d.-thesis, IMT.
IMT 2009-56	Ayala-Uraga, Efren	Reliability-Based Assessment of Deteriorating Ship-shaped Offshore Structures, Ph.d.-thesis, IMT
IMT 2009-57	Kong, Xiangjun	A Numerical Study of a Damaged Ship in Beam Sea Waves. Ph.d.-thesis, IMT/CeSOS.
IMT 2010-58	Kristiansen, David	Wave Induced Effects on Floaters of Aquaculture Plants, Ph.d.-thesis, CeSOS.
IMT 2010-59	Ludvigsen, Martin	An ROV-Toolbox for Optical and Acoustic Scientific Seabed Investigation. Ph.d.-thesis IMT.
IMT 2010-60	Hals, Jørgen	Modelling and Phase Control of Wave-Energy Converters. Ph.d.thesis, CeSOS.

IMT 2010- 61	Shu, Zhi	Uncertainty Assessment of Wave Loads and Ultimate Strength of Tankers and Bulk Carriers in a Reliability Framework. Ph.d. Thesis, IMT/ CeSOS
IMT 2010-62	Shao, Yanlin	Numerical Potential-Flow Studies on Weakly-Nonlinear Wave-Body Interactions with/without Small Forward Speed, Ph.d.thesis,CeSOS.
IMT 2010-63	Califano, Andrea	Dynamic Loads on Marine Propellers due to Intermittent Ventilation. Ph.d.thesis, IMT.
IMT 2010-64	El Khoury, George	Numerical Simulations of Massively Separated Turbulent Flows, Ph.d.-thesis, IMT
IMT 2010-65	Seim, Knut Sponheim	Mixing Process in Dense Overflows with Emphasis on the Faroe Bank Channel Overflow. Ph.d.thesis, IMT
IMT 2010-66	Jia, Huirong	Structural Analysis of Intect and Damaged Ships in a Collission Risk Analysis Perspective. Ph.d.thesis CeSoS.
IMT 2010-67	Jiao, Linlin	Wave-Induced Effects on a Pontoon-type Very Large Floating Structures (VLFS). Ph.D.-thesis, CeSOS.
IMT 2010-68	Abrahamsen, Bjørn Christian	Sloshing Induced Tank Roof with Entrapped Air Pocket. Ph.d.thesis, CeSOS.
IMT 2011-69	Karimirad, Madjid	Stochastic Dynamic Response Analysis of Spar-Type Wind Turbines with Catenary or Taut Mooring Systems. Ph.d.-thesis, CeSOS.
IMT - 2011-70	Erlend Meland	Condition Monitoring of Safety Critical Valves. Ph.d.-thesis, IMT.
IMT – 2011-71	Yang, Limin	Stochastic Dynamic System Analysis of Wave Energy Converter with Hydraulic Power Take-Off, with Particular Reference to Wear Damage Analysis, Ph.d. Thesis, CeSOS.
IMT – 2011-72	Visscher, Jan	Application of Particla Image Velocimetry on Turbulent Marine Flows, Ph.d.Thesis, IMT.
IMT – 2011-73	Su, Biao	Numerical Predictions of Global and Local Ice Loads on Ships. Ph.d.Thesis, CeSOS.
IMT – 2011-74	Liu, Zhenhui	Analytical and Numerical Analysis of Iceberg Collision with Ship Structures. Ph.d.Thesis, IMT.
IMT – 2011-75	Aarsæther, Karl Gunnar	Modeling and Analysis of Ship Traffic by Observation and Numerical Simulation. Ph.d.Thesis, IMT.
Imt – 2011-76	Wu, Jie	Hydrodynamic Force Identification from Stochastic Vortex Induced Vibration Experiments with Slender Beams. Ph.d.Thesis, IMT.

Imt – 2011-77	Amini, Hamid	Azimuth Propulsors in Off-design Conditions. Ph.d.Thesis, IMT.
IMT – 2011-78	Nguyen, Tan-Hoi	Toward a System of Real-Time Prediction and Monitoring of Bottom Damage Conditions During Ship Grounding. Ph.d.thesis, IMT.
IMT- 2011-79	Tavakoli, Mohammad T.	Assessment of Oil Spill in Ship Collision and Grounding, Ph.d.thesis, IMT.
IMT- 2011-80	Guo, Bingjie	Numerical and Experimental Investigation of Added Resistance in Waves. Ph.d.Thesis, IMT.
IMT- 2011-81	Chen, Qiaofeng	Ultimate Strength of Aluminium Panels, considering HAZ Effects, IMT
IMT- 2012-82	Kota, Ravikiran S.	Wave Loads on Decks of Offshore Structures in Random Seas, CeSOS.
IMT- 2012-83	Sten, Ronny	Dynamic Simulation of Deep Water Drilling Risers with Heave Compensating System, IMT.
IMT- 2012-84	Berle, Øyvind	Risk and resilience in global maritime supply chains, IMT.
IMT- 2012-85	Fang, Shaoji	Fault Tolerant Position Mooring Control Based on Structural Reliability, CeSOS.
IMT- 2012-86	You, Jikun	Numerical studies on wave forces and moored ship motions in intermediate and shallow water, CeSOS.
IMT- 2012-87	Xiang ,Xu	Maneuvering of two interacting ships in waves, CeSOS
IMT- 2012-88	Dong, Wenbin	Time-domain fatigue response and reliability analysis of offshore wind turbines with emphasis on welded tubular joints and gear components, CeSOS
IMT- 2012-89	Zhu, Suji	Investigation of Wave-Induced Nonlinear Load Effects in Open Ships considering Hull Girder Vibrations in Bending and Torsion, CeSOS
IMT- 2012-90	Zhou, Li	Numerical and Experimental Investigation of Station-keeping in Level Ice, CeSOS
IMT- 2012-91	Ushakov, Sergey	Particulate matter emission characteristics from diesel enignes operating on conventional and alternative marine fuels, IMT
IMT- 2013-1	Yin, Decao	Experimental and Numerical Analysis of Combined In-line and Cross-flow Vortex Induced Vibrations, CeSOS
IMT- 2013-2	Kurniawan, Adi	Modelling and geometry optimisation of wave energy converters, CeSOS

IMT-2013-3	Al Ryati, Nabil	Technical condition indexes doe auxiliary marine diesel engines, IMT
IMT-2013-4	Firoozkoohi, Reza	Experimental, numerical and analytical investigation of the effect of screens on sloshing, CeSOS
IMT-2013-5	Ommani, Babak	Potential-Flow Predictions of a Semi-Displacement Vessel Including Applications to Calm Water Broaching, CeSOS
IMT-2013-6	Xing, Yihan	Modelling and analysis of the gearbox in a floating spar-type wind turbine, CeSOS
IMT-7-2013	Balland, Océane	Optimization models for reducing air emissions from ships, IMT
IMT-8-2013	Yang, Dan	Transitional wake flow behind an inclined flat plate-----Computation and analysis, IMT
IMT-9-2013	Abdillah, Suyuthi	Prediction of Extreme Loads and Fatigue Damage for a Ship Hull due to Ice Action, IMT
IMT-10-2013	Ramìrez, Pedro Agustìn Pèrez	Ageing management and life extension of technical systems- Concepts and methods applied to oil and gas facilities, IMT
IMT-11-2013	Chuang, Zhenju	Experimental and Numerical Investigation of Speed Loss due to Seakeeping and Maneuvering. IMT
IMT-12-2013	Etemaddar, Mahmoud	Load and Response Analysis of Wind Turbines under Atmospheric Icing and Controller System Faults with Emphasis on Spar Type Floating Wind Turbines, IMT
IMT-13-2013	Lindstad, Haakon	Strategies and measures for reducing maritime CO2 emissons, IMT
IMT-14-2013	Haris, Sabril	Damage interaction analysis of ship collisions, IMT
IMT-15-2013	Shainee, Mohamed	Conceptual Design, Numerical and Experimental Investigation of a SPM Cage Concept for Offshore Mariculture, IMT
IMT-16-2013	Gansel, Lars	Flow past porous cylinders and effects of biofouling and fish behavior on the flow in and around Atlantic salmon net cages, IMT
IMT-17-2013	Gaspar, Henrique	Handling Aspects of Complexity in Conceptual Ship Design, IMT
IMT-18-2013	Thys, Maxime	Theoretical and Experimental Investigation of a Free Running Fishing Vessel at Small Frequency of Encounter, CeSOS
IMT-19-2013	Aglen, Ida	VIV in Free Spanning Pipelines, CeSOS
IMT-1-2014	Song, An	Theoretical and experimental studies of wave diffraction and radiation loads on a horizontally submerged perforated plate, CeSOS

IMT-2-2014	Rogne, Øyvind Ygre	Numerical and Experimental Investigation of a Hinged 5-body Wave Energy Converter, CeSOS
IMT-3-2014	Dai, Lijuan	Safe and efficient operation and maintenance of offshore wind farms ,IMT
IMT-4-2014	Bachynski, Erin Elizabeth	Design and Dynamic Analysis of Tension Leg Platform Wind Turbines, CeSOS
IMT-5-2014	Wang, Jingbo	Water Entry of Freefall Wedged – Wedge motions and Cavity Dynamics, CeSOS
IMT-6-2014	Kim, Ekaterina	Experimental and numerical studies related to the coupled behavior of ice mass and steel structures during accidental collisions, IMT
IMT-7-2014	Tan, Xiang	Numerical investigation of ship's continuous- mode icebreaking in leverl ice, CeSOS
IMT-8-2014	Muliawan, Made Jaya	Design and Analysis of Combined Floating Wave and Wind Power Facilities, with Emphasis on Extreme Load Effects of the Mooring System, CeSOS
IMT-9-2014	Jiang, Zhiyu	Long-term response analysis of wind turbines with an emphasis on fault and shutdown conditions, IMT
IMT-10-2014	Dukan, Fredrik	ROV Motion Control Systems, IMT
IMT-11-2014	Grimsmo, Nils I.	Dynamic simulations of hydraulic cylinder for heave compensation of deep water drilling risers, IMT
IMT-12-2014	Kvittem, Marit I.	Modelling and response analysis for fatigue design of a semisubmersible wind turbine, CeSOS
IMT-13-2014	Akhtar, Juned	The Effects of Human Fatigue on Risk at Sea, IMT
IMT-14-2014	Syahroni, Nur	Fatigue Assessment of Welded Joints Taking into Account Effects of Residual Stress, IMT
IMT-1-2015	Bøckmann, Eirik	Wave Propulsion of ships, IMT
IMT-2-2015	Wang, Kai	Modelling and dynamic analysis of a semi-submersible floating vertical axis wind turbine, CeSOS
IMT-3-2015	Fredriksen, Arnt Gunvald	A numerical and experimental study of a two-dimensional body with moonpool in waves and current, CeSOS
IMT-4-2015	Jose Patricio Gallardo Canabes	Numerical studies of viscous flow around bluff bodies, IMT
IMT-5-2015	Vegard Longva	Formulation and application of finite element techniques for slender marine structures subjected to contact interactions, IMT

IMT-6-2015	Jacobus De Vaal	Aerodynamic modelling of floating wind turbines, CeSOS
IMT-7-2015	Fachri Nasution	Fatigue Performance of Copper Power Conductors, IMT
IMT-8-2015	Oleh I Karpa	Development of bivariate extreme value distributions for applications in marine technology,CeSOS
IMT-9-2015	Daniel de Almeida Fernandes	An output feedback motion control system for ROVs, AMOS
IMT-10-2015	Bo Zhao	Particle Filter for Fault Diagnosis: Application to Dynamic Positioning Vessel and Underwater Robotics, CeSOS
IMT-11-2015	Wenting Zhu	Impact of emission allocation in maritime transportation, IMT
IMT-12-2015	Amir Rasekhi Nejad	Dynamic Analysis and Design of Gearboxes in Offshore Wind Turbines in a Structural Reliability Perspective, CeSOS
IMT-13-2015	Arturo Jesùs Ortega Malca	Dynamic Response of Flexibles Risers due to Unsteady Slug Flow, CeSOS
IMT-14-2015	Dagfinn Husjord	Guidance and decision-support system for safe navigation of ships operating in close proximity, IMT
IMT-15-2015	Anirban Bhattacharyya	Ducted Propellers: Behaviour in Waves and Scale Effects, IMT
IMT-16-2015	Qin Zhang	Image Processing for Ice Parameter Identification in Ice Management, IMT
IMT-1-2016	Vincentius Rumawas	Human Factors in Ship Design and Operation: An Experiential Learning, IMT
IMT-2-2016	Martin Storheim	Structural response in ship-platform and ship-ice collisions, IMT
IMT-3-2016	Mia Abrahamsen Prsic	Numerical Simulations of the Flow around single and Tandem Circular Cylinders Close to a Plane Wall, IMT
IMT-4-2016	Tufan Arslan	Large-eddy simulations of cross-flow around ship sections, IMT
IMT-5-2016	Pierre Yves-Henry	Parametrisation of aquatic vegetation in hydraulic and coastal research,IMT
IMT-6-2016	Lin Li	Dynamic Analysis of the Instalation of Monopiles for Offshore Wind Turbines, CeSOS

IMT-7-2016	Øivind Kåre Kjerstad	Dynamic Positioning of Marine Vessels in Ice, IMT
IMT-8-2016	Xiaopeng Wu	Numerical Analysis of Anchor Handling and Fish Trawling Operations in a Safety Perspective, CeSOS
IMT-9-2016	Zhengshun Cheng	Integrated Dynamic Analysis of Floating Vertical Axis Wind Turbines, CeSOS
IMT-10-2016	Ling Wan	Experimental and Numerical Study of a Combined Offshore Wind and Wave Energy Converter Concept
IMT-11-2016	Wei Chai	Stochastic dynamic analysis and reliability evaluation of the roll motion for ships in random seas, CeSOS
IMT-12-2016	Øyvind Selnes Patricksson	Decision support for conceptual ship design with focus on a changing life cycle and future uncertainty, IMT
IMT-13-2016	Mats Jørgen Thorsen	Time domain analysis of vortex-induced vibrations, IMT
IMT-14-2016	Edgar McGuinness	Safety in the Norwegian Fishing Fleet – Analysis and measures for improvement, IMT
IMT-15-2016	Sepideh Jafarzadeh	Energy effiency and emission abatement in the fishing fleet, IMT
IMT-16-2016	Wilson Ivan Guachamin Acero	Assessment of marine operations for offshore wind turbine installation with emphasis on response-based operational limits, IMT
IMT-17-2016	Mauro Candeloro	Tools and Methods for Autonomous Operations on Seabed and Water Coumn using Underwater Vehicles, IMT
IMT-18-2016	Valentin Chabaud	Real-Time Hybrid Model Testing of Floating Wind Tubines, IMT
IMT-1-2017	Mohammad Saud Afzal	Three-dimensional streaming in a sea bed boundary layer
IMT-2-2017	Peng Li	A Theoretical and Experimental Study of Wave-induced Hydroelastic Response of a Circular Floating Collar
IMT-3-2017	Martin Bergström	A simulation-based design method for arctic maritime transport systems
IMT-4-2017	Bhushan Taskar	The effect of waves on marine propellers and propulsion
IMT-5-2017	Mohsen Bardestani	A two-dimensional numerical and experimental study of a floater with net and sinker tube in waves and current

IMT-6-2017	Fatemeh Hoseini Dadmarzi	Direct Numerical Simualtion of turbulent wakes behind different plate configurations
IMT-7-2017	Michel R. Miyazaki	Modeling and control of hybrid marine power plants
IMT-8-2017	Giri Rajasekhar Gunnu	Safety and effiency enhancement of anchor handling operations with particular emphasis on the stability of anchor handling vessels
IMT-9-2017	Kevin Koosup Yum	Transient Performance and Emissions of a Turbocharged Diesel Engine for Marine Power Plants
IMT-10-2017	Zhaolong Yu	Hydrodynamic and structural aspects of ship collisions
IMT-11-2017	Martin Hassel	Risk Analysis and Modelling of Allisions between Passing Vessels and Offshore Installations
IMT-12-2017	Astrid H. Brodtkorb	Hybrid Control of Marine Vessels – Dynamic Positioning in Varying Conditions
IMT-13-2017	Kjersti Bruserud	Simultaneous stochastic model of waves and current for prediction of structural design loads
IMT-14-2017	Finn-Idar Grøtta Giske	Long-Term Extreme Response Analysis of Marine Structures Using Inverse Reliability Methods
IMT-15-2017	Stian Skjong	Modeling and Simulation of Maritime Systems and Operations for Virtual Prototyping using co-Simulations
IMT-1-2018	Yingguang Chu	Virtual Prototyping for Marine Crane Design and Operations
IMT-2-2018	Sergey Gavrilin	Validation of ship manoeuvring simulation models
IMT-3-2018	Jeevith Hegde	Tools and methods to manage risk in autonomous subsea inspection,maintenance and repair operations
IMT-4-2018	Ida M. Strand	Sea Loads on Closed Flexible Fish Cages
IMT-5-2018	Erlend Kvinge Jørgensen	Navigation and Control of Underwater Robotic Vehicles
IMT-6-2018	Bård Stovner	Aided Intertial Navigation of Underwater Vehicles
IMT-7-2018	Erlend Liavåg Grotle	Thermodynamic Response Enhanced by Sloshing in Marine LNG Fuel Tanks

IMT-8-2018	Børge Rokseth	Safety and Verification of Advanced Maritime Vessels
IMT-9-2018	Jan Vidar Ulveseter	Advances in Semi-Empirical Time Domain Modelling of Vortex-Induced Vibrations
IMT-10-2018	Chenyu Luan	Design and analysis for a steel braceless semi-submersible hull for supporting a 5-MW horizontal axis wind turbine
IMT-11-2018	Carl Fredrik Rehn	Ship Design under Uncertainty
IMT-12-2018	Øyvind Ødegård	Towards Autonomous Operations and Systems in Marine Archaeology
IMT-13-2018	Stein Melvær Nornes	Guidance and Control of Marine Robotics for Ocean Mapping and Monitoring
IMT-14-2018	Petter Norgren	Autonomous Underwater Vehicles in Arctic Marine Operations: Arctic marine research and ice monitoring
IMT-15-2018	Minjoo Choi	Modular Adaptable Ship Design for Handling Uncertainty in the Future Operating Context
MT-16-2018	Ole Alexander Eidsvik	Dynamics of Remotely Operated Underwater Vehicle Systems
IMT-17-2018	Mahdi Ghane	Fault Diagnosis of Floating Wind Turbine Drivetrain- Methodologies and Applications
IMT-18-2018	Christoph Alexander Thieme	Risk Analysis and Modelling of Autonomous Marine Systems
IMT-19-2018	Yugao Shen	Operational limits for floating-collar fish farms in waves and current, without and with well-boat presence
IMT-20-2018	Tianjiao Dai	Investigations of Shear Interaction and Stresses in Flexible Pipes and Umbilicals
IMT-21-2018	Sigurd Solheim Pettersen	Resilience by Latent Capabilities in Marine Systems
IMT-22-2018	Thomas Sauder	Fidelity of Cyber-physical Empirical Methods. Application to the Active Truncation of Slender Marine Structures
IMT-23-2018	Jan-Tore Horn	Statistical and Modelling Uncertainties in the Design of Offshore Wind Turbines
IMT-24-2018	Anna Swider	Data Mining Methods for the Analysis of Power Systems of Vessels
IMT-1-2019	Zhao He	Hydrodynamic study of a moored fish farming cage with fish influence

IMT-2-2019	Isar Ghamari	Numerical and Experimental Study on the Ship Parametric Roll Resonance and the Effect of Anti-Roll Tank
IMT-3-2019	Håkon Strandenes	Turbulent Flow Simulations at Higher Reynolds Numbers
IMT-4-2019	Siri Mariane Holen	Safety in Norwegian Fish Farming – Concepts and Methods for Improvement
IMT-5-2019	Ping Fu	Reliability Analysis of Wake-Induced Riser Collision
IMT-6-2019	Vladimir Krivopolianskii	Experimental Investigation of Injection and Combustion Processes in Marine Gas Engines using Constant Volume Rig
IMT-7-2019	Anna Maria Kozlowska	Hydrodynamic Loads on Marine Propellers Subject to Ventilation and out of Water Condition.
IMT-8-2019	Hans-Martin Heyn	Motion Sensing on Vessels Operating in Sea Ice: A Local Ice Monitoring System for Transit and Stationkeeping Operations under the Influence of Sea Ice
IMT-9-2019	Stefan Vilsen	Method for Real-Time Hybrid Model Testing of Ocean Structures – Case on Slender Marine Systems
IMT-10-2019	Finn-Christian W. Hanssen	Non-Linear Wave-Body Interaction in Severe Waves
IMT-11-2019	Trygve Olav Fossum	Adaptive Sampling for Marine Robotics
IMT-12-2019	Jørgen Bremnes Nielsen	Modeling and Simulation for Design Evaluation
IMT-13-2019	Yuna Zhao	Numerical modelling and dyncamic analysis of offshore wind turbine blade installation
IMT-14-2019	Daniela Myland	Experimental and Theoretical Investigations on the Ship Resistance in Level Ice
IMT-15-2019	Zhengru Ren	Advanced control algorithms to support automated offshore wind turbine installation
IMT-16-2019	Drazen Polic	Ice-propeller impact analysis using an inverse propulsion machinery simulation approach
IMT-17-2019	Endre Sandvik	Sea passage scenario simulation for ship system performance evaluation
IMT-18-2019	Loup Suja-Thauvin	Response of Monopile Wind Turbines to Higher Order Wave Loads
IMT-19-2019	Emil Smilden	Structural control of offshore wind turbines – Increasing the role of control design in offshore wind farm development

IMT-20-2019	Aleksandar-Sasa Milakovic	On equivalent ice thickness and machine learning in ship ice transit simulations
IMT-1-2020	Amrit Shankar Verma	Modelling, Analysis and Response-based Operability Assessment of Offshore Wind Turbine Blade Installation with Emphasis on Impact Damages
IMT-2-2020	Bent Oddvar Arnesen Haugaløkken	Autonomous Technology for Inspection, Maintenance and Repair Operations in the Norwegian Aquaculture
IMT-3-2020	Seongpil Cho	Model-based fault detection and diagnosis of a blade pitch system in floating wind turbines
IMT-4-2020	Jose Jorge Garcia Agis	Effectiveness in Decision-Making in Ship Design under Uncertainty
IMT-5-2020	Thomas H. Viuff	Uncertainty Assessment of Wave-and Current-induced Global Response of Floating Bridges
IMT-6-2020	Fredrik Mentzoni	Hydrodynamic Loads on Complex Structures in the Wave Zone
IMT-7-2020	Senthuran Ravinthrakumar	Numerical and Experimental Studies of Resonant Flow in Moonpools in Operational Conditions
IMT-8-2020	Stian Skaalvik Sandøy	Acoustic-based Probabilistic Localization and Mapping using Unmanned Underwater Vehicles for Aquaculture Operations
IMT-9-2020	Kun Xu	Design and Analysis of Mooring System for Semi-submersible Floating Wind Turbine in Shallow Water
IMT-10-2020	Jianxun Zhu	Cavity Flows and Wake Behind an Elliptic Cylinder Translating Above the Wall
IMT-11-2020	Sandra Hogenboom	Decision-making within Dynamic Positioning Operations in the Offshore Industry – A Human Factors based Approach
IMT-12-2020	Woongshik Nam	Structural Resistance of Ship and Offshore Structures Exposed to the Risk of Brittle Failure
IMT-13-2020	Svenn Are Tutturen Værnø	Transient Performance in Dynamic Positioning of Ships: Investigation of Residual Load Models and Control Methods for Effective Compensation
IMT-14-2020	Mohd Atif Siddiqui	Experimental and Numerical Hydrodynamic Analysis of a Damaged Ship in Waves
IMT-15-2020	John Marius Hegseth	Efficient Modelling and Design Optimization of Large Floating Wind Turbines
IMT-16-2020	Asle Natskår	Reliability-based Assessment of Marine Operations with Emphasis on Sea Transport on Barges

IMT-17-2020	Shi Deng	Experimental and Numerical Study of Hydrodynamic Responses of a Twin-Tube Submerged Floating Tunnel Considering Vortex-Induced Vibration
IMT-18-2020	Jone Torsvik	Dynamic Analysis in Design and Operation of Large Floating Offshore Wind Turbine Drivetrains
IMT-1-2021	Ali Ebrahimi	Handling Complexity to Improve Ship Design Competitiveness
IMT-2-2021	Davide Proserpio	Isogeometric Phase-Field Methods for Modeling Fracture in Shell Structures
IMT-3-2021	Cai Tian	Numerical Studies of Viscous Flow Around Step Cylinders
IMT-4-2021	Farid Khazaeli Moghadam	Vibration-based Condition Monitoring of Large Offshore Wind Turbines in a Digital Twin Perspective
IMT-5-2021	Shuaishuai Wang	Design and Dynamic Analysis of a 10-MW Medium-Speed Drivetrain in Offshore Wind Turbines
IMT-6-2021	Sadi Tavakoli	Ship Propulsion Dynamics and Emissions
IMT-7-2021	Haoran Li	Nonlinear wave loads, and resulting global response statistics of a semi-submersible wind turbine platform with heave plates
IMT-8-2021	Einar Skiftestad Ueland	Load Control for Real-Time Hybrid Model Testing using Cable-Driven Parallel Robots
IMT-9-2021	Mengning Wu	Uncertainty of machine learning-based methods for wave forecast and its effect on installation of offshore wind turbines
IMT-10-2021	Xu Han	Onboard Tuning and Uncertainty Estimation of Vessel Seakeeping Model Parameters
IMT-01-2022	Ingunn Marie Holmen	Safety in Exposed Aquacultrue Operations
IMT-02-2022	Prateek Gupta	Ship Performance Monitoring using In-service Measurements and Big Data Analysis Methods
IMT-03-2022	Sangwoo Kim	Non-linear time domain analysis of deepwater riser vortex-induced vibrations
IMT-04-2022	Jarle Vinje Kramer	Hydrodynamic Aspects of Sail-Assisted Merchant Vessels
IMT-05-2022	Øyvind Rabliås	Numerical and Expermental Studies of Maneuvering in Regular and Irregular Waves
IMT-06-2022	Pramod Ghimire	Simulation-Based Ship Hybrid Power System Conspet Studies and Performance Analyses

IMT-07-2022	Carlos Eduardo Silva de Souza	Structural modelling, coupled dynamics, and design of large floating wind turbines
IMT-08-2022	Lorenzo Balestra	Design of hybrid fuel cell & battery systems for maritime vessels
IMT-09-2022	Sharmin Sultana	Process safety and risk management using system perspectives – A contribution to the chemical process and petroleum industry