



Risk Analysis Applied to Integrate Safety and Security into Systems Design

Svana Helen Björnsdóttir

May 2024

Department of Engineering

Reykjavík University

Ph.D. Dissertation



Risk Analysis Applied to Integrate Safety and Security into Systems Design

Dissertation submitted to the Department of Engineering, School of Technology at Reykjavík University in partial fulfillment of the requirements for the degree of **Doctor of Philosophy (Ph.D.)**

May 2024

Thesis Committee:

Páll Jensson, Ph.D.

Professor Emeritus, Reykjavik University, Iceland
Thesis Committee Chair

Ioannis M. Dokas, Ph.D.

Assistant Professor, Democritus University of Thrace, Greece

Nancy G. Leveson, Ph.D.

Professor, Massachusetts Institute of Technology, USA

Robert Jan de Boer, Ph.D.

Professor, SDO University of Applied Sciences, The Netherlands

Borgeir Pálsson, Ph.D.

Professor Emeritus, Reykjavik University, Iceland

Examiners:

Floris Goerlandt, Ph.D.

Associate Professor, Dalhousie University, Canada

Gunnar Stefánsson, Ph.D.

Professor, University of Iceland, Iceland

Copyright © 2024 Svana Helen Björnsdóttir
All rights reserved.

The author hereby grants permission to the Reykjavík University Library to reproduce single copies of this Dissertation entitled *Risk Analysis Applied to Integrate Safety and Security into Systems Design* and to lend or sell such copies for private, scholarly, or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the Dissertation, and except as herein before provided, neither the Dissertation nor any substantial portion thereof may be printed or otherwise reproduced in any material form whatsoever without the author's prior written permission.

ISBN 978-9935-539-31-1 Electronic version
ISBN 978-9935-539-30-4 Print version

ORCID Svana Helen Björnsdóttir 0000-0003-2120-3897
<https://orcid.org/0000-0003-2120-3897>

Risk Analysis Applied to Integrate Safety and Security into Systems Design

Svana Helen Björnsdóttir

Abstract

The overall aim of this Ph.D. thesis is to contribute to the further development of the research area of risk analysis and risk management. It aims to bridge the gap between scientific research in this area and its practical application in industry and business, e.g., through the development of ISO standards. Industrial standards, notably ISO standards, are the tools organizations use to manage their risk, by following their guidance and complying with their requirements. Organizations confirm their compliance with these standards through certification, which means that they heavily depend on the quality of the ISO standards to enable them to effectively manage risk.

In this thesis, the scientific foundation of ISO standards is analyzed, focusing on the guidance provided for key elements of risk management. The research also explores how well ISO standards are aligned with state-of-the-art risk management literature. The research reveals that the ISO standards lack uniformity in risk terminology and guidance on risk management, particularly for risk analysis. As a result, it is expected that risk management, and specifically the analysis of risk, is not executed satisfactorily. Therefore, it is hypothesized that certain flaws in risk management will be evident in practice. This is verified through six real-life case study examples.

Part of this thesis work involved developing a two-step benchmarking model to assess the efficacy of ISO risk management systems with the aim of finding hidden risk issues and improvement opportunities. Furthermore, it is investigated whether risk analysis can be improved by using new and improved analysis techniques to identify hazards and threats. The thesis explores the application of recent analysis techniques that are based on systems theory to reinforce risk management systems based on ISO standards. Systems-Theoretic Accident Model and Processes (STAMP), and the derived Systems-Theoretic Process Analysis (STPA) and Systems-Theoretic Early Concept Analysis (STECA) are applied in real case studies and in an early phase of a major national infrastructure project to meet the safe-by-design engineering concept.

The main contribution of this Ph.D. thesis is the identification of what is missing in ISO standards regarding risk management and the development of a two-step benchmarking model to assess the efficacy of ISO risk management systems. The research demonstrates how it is possible to improve risk identification and risk analysis with STAMP, STPA, and STECA techniques. To facilitate such analysis, a special STAMP/STPA software was developed as a part of this thesis work.

Áhættugreiningu beitt til að samþætta öryggi við hönnun kerfa

Svana Helen Björnsdóttir

Útdráttur

Meginmarkmið þessarar doktorsritgerðar er að stuðla að frekari þróun innan rannsóknarsviðs áhættugreiningar og áhættustjórnunar. Hún miðar að því að brúa bilið sem er á milli vísindarannsókna á þessu sviði og hagnýtingar þeirra í iðnaði og viðskiptum, t.d. í gegnum þróun ISO-staðla. Iðnaðarstaðlar, sérstaklega ISO-staðlar, eru þau tæki sem fyrirtæki og stofnanir beita til að stjórna áhættu í rekstri, með því að fylgja leiðbeiningum og fara eftir kröfum þeirra. Fyrirtæki og stofnanir staðfesta að þau uppfylli þessa staðla með vottun, sem þýðir að þau eru mjög háð gæðum ISO-staðlanna til að gera þeim kleift að stjórna áhættu á áhrifaríkan hátt.

Í þessari ritgerð er vísindalegur grunnur ISO-staðla rannsakaður og sjónum sérstaklega beint að leiðbeiningum sem veittar eru í stöðlunum um lykilþætti áhættustjórnunar. Í ritgerðinni er ennfremur kannað hversu vel ISO-staðlar samræmast nýjustu vísindarannsóknum á sviði áhættustjórnunar. Rannsóknin leiðir í ljós að ISO-staðlana skortir samræmda hugtakanotkun í leiðbeiningum um áhættustjórnun, sérstaklega er varðar áhættugreiningu. Þess vegna er sett fram sú tilgáta að áhættustjórnun og þá sérstaklega greining áhættu sé ekki framkvæmd á fullnægjandi hátt og að ákveðnar veilur komi fram við framkvæmd áhættustjórnunar í reynd. Þetta er sannreynt með sex dæmum úr raunverulegum rekstri.

Hluti af þessari rannsókn fólst í því að þróa tveggja þrepa viðmiðunarlíkan til að meta virkni ISO-áhættustjórnunarkerfa með það að markmiði að finna dulda áhættuþætti og umbótataækifæri. Í tengslum við það er rannsakað hvort bæta megi áhættugreiningu með því að nota nýja og endurbætta greiningartækni til að greina hættur og ógnir. Ritgerðin fjallar um beitingu nýlegrar greiningartækni sem byggir á kerfisfræði til að styrkja áhættustjórnunarkerfi byggð á ISO-stöðlum. Beitt er kerfisfræðilegri aðferð sem byggist á gerð slysalíkans og greiningu verkferla, á ensku nefnd „Systems-Theoretic Accident Model and Processes“ (STAMP) og afleiddri kerfisfræðilegri aðferðagreiningu sem á ensku er nefnd „Systems-Theoretic Process Analysis“ (STPA)

ásamt kerfisfræðilegri snemmgreiningu sem á ensku er nefnd „Systems-Theoretic Early Concept Analysis“ (STECA). Þessum aðferðum er beitt í raunverulegum tilviksrannsóknum og enn fremur á frumstigi stórs innviðaverkefnis á landsvísu í þeim tilgangi að uppfylla verkfræðihugmynd um örugga hönnun. Meginframlag þessarar doktorsritgerðar er að bera kennsl á það sem vantar í ISO-staðla varðandi áhættustjórnun og sýna fram á leiðir til að bæta og styrkja áhættustjórnkerfi sem byggja á slíkum stöðlum. Rannsóknin sýnir hvernig hægt er að bæta árangur við það að bera kennsl á áhættu og greina hana með STAMP, STPA og STECA tækni. Til að auðvelda slíka greiningu var sérstakur STAMP/STPA hugbúnaður þróaður sem hluti af þessari rannsókn.

*I dedicate this dissertation to the memory of my father,
Björn Hafsteinn Jóhannsson (June 4, 1939 – August 31, 2011),
a mechanical engineer,
for sparking my interest in engineering.*

Acknowledgements

The Ph.D. Journey

This research started formally in 2014 when the research application was accepted by the School of Science and Engineering at Reykjavik University. The research proceeded as planned at first. Written agreements were made and signed with six ISO certified organizations that had agreed to participate in the research. Their role was to provide information regarding their risk analysis, risk assessment and risk management processes. The agreements are in line with ISO 27001 and include confidentiality requirements so that the publication of results regarding participants is subject to the consent of the participants.

The initial plan was to conduct a literature review on the definition of risk terms and risk analysis, both in scientific articles and in ISO standards. Then six case studies would be carried out at ISO certified organizations that all perform a risk analysis according to documented risk management processes. An article would be written about the results of these case studies. Finally, the Systems-Theoretic Accident Model and Processes (STAMP) and the derived Systems-Theoretic Process Analysis (STPA) technique would be applied to analyze hazards, threats, and risk for the same six cases and 3-6 articles would be written about the results. It was assumed that the study would take at least five years, since the research was done part-time along with other jobs and assignments.

The first article took longer to process than initially planned, i.e., because at this time the importance of ISO standards was changing in such a way that risk management is now required in all ISO management standards. Finally, when the draft of the first article was ready, it was sent to a publisher in 2016. After nine months of waiting the article was rejected. This led to a delay in the research and the writing of more articles. When the rejection finally came the paper was rewritten and sent to another publisher, Risk Analysis, and first published in September 2021. Meanwhile, the research continued with case studies, which consisted of a quantitative research component in the form of a questionnaire and a qualitative component in the form of in-depth interviews. STAMP/STPA workshops and conferences were attended twice a year, and the first results were presented in those conferences, see a list of conference presentations in Section 4.6.1.

An opportunity arose for cooperation in the development of specialized STPA software to facilitate the research work. A proposal for a three-year Eurostars project was submitted and a grant received in 2017. The software was developed in collaboration between the software company Stiki ehf. in Reykjavík and the Zürich University for applied technologies (ZHAW). The author of this Dissertation was the project manager of this project and led both application writing and development to the end, in 2019. The STPA software, which is the result of the spin-off project of this research, has been of good use in this project and has also been sold to customers around the world. The first article presented as a part of this thesis work was a conference paper, marked as Article D in the list of articles in chapter 4.4.

During the whole research process there has been an active participation in international STAMP/STPA conferences and workshops. Until COVID a physical four-day workshop and conference was held annually in March at MIT and organized by Professor Nancy Leveson. A similar three-day workshop has been held annually in Europe since 2013. Both conferences were regularly attended. In 2017 the Fifth European STAMP/STPA Workshop and

Conference (ESWC) was held at Reykjavik University, organized by the author of this Dissertation with support from Professor Páll Jensson, Dr. Þórður Víkingur Friðgeirsson and other colleagues at Reykjavik University – and with support from the European ESWC Steering Group. COVID changed these workshops and conferences into virtual events on a smaller scale.

An opportunity arose within Reykjavik University to participate in research on the application of the VUCA meter, that stands for Volatility, Uncertainty, Complexity, and Ambiguity. VUCA is a project risk identification process different from STAMP/STPA. The VUCA meter describes the situation of constant, unpredictable change that has now become the norm in certain industries and areas of the business world. See Article E in chapter 4.5.

When writing Article B that presents the results from the six case studies, it became clear that despite declarations and consent on the participants' behalf to publish the results, there was a great reluctance to do so. It took half a year to get approval for the publication of the results in the article, and much time was spent discussing the wording and rephrasing of the text. It then became clear that consent would not be obtained for the publication of more detailed results, which participants believed would disclose too much sensitive information regarding their vulnerability and risk.

After a meeting with Professor Páll Jensson, the main supervisor in this thesis work, it was decided to add a Systems-Theoretic Early Concept Analysis (STECA) of a project that has not yet commenced and has no project owner. STECA is a variation of STPA and based on STAMP. The project chosen for this analysis is a major infrastructure project now under consideration in Iceland, a national Waste-to-Energy (WtE) incineration plant for all of Iceland that would make the country sustainable in terms of waste management. The publication of this work cannot be hindered, and the results can be useful in decision making and preparation of the project, if realized. Article C presents the results of the analysis.

Professor Páll Jensson took me under his wing on this Ph.D. journey from the beginning. As the advisor and committee chair, he not only guided the research, but also nurtured the ability to conduct original research and to communicate ideas and results more articulately. Professor Páll Jensson, a special thanks to you for all your time and support during my Ph.D. journey and in developing my research abilities.

The Ph.D. committee consisted of top professionals in their field. My research benefitted immensely from their on-point feedback, knowledge, and intellectual curiosity. I am grateful for their time, energy, and guidance.

Professor Nancy G. Leveson, thank you for opening the door to STAMP, STPA, and STECA for me, for your MIT workshops, for your guidance, and your incredible energy and enthusiasm.

Professor Ioannis M Dokas, thank you for your support, for the encouragement, for your guidance, and for sharing your expertise in STAMP, STPA, and STECA. Thank you also for your valuable feedback and all the good discussions we had on Teams, both during and after COVID-19.

Professor Robert Jan de Boer, thank you for sharing with me your expertise in both engineering and social sciences, for your time and probing questions. Thank you also for the fruitful discussions we had along the way.

Professor Þorgeir Pálsson, thank you for your encouragement, thorough review, for your time and listening, and giving feedback to research ideas.

In addition to the formal committee, many others were involved. Master students at

Reykjavik University and MIT took part in my Ph.D. through their master theses and case studies: Helga Einarsdóttir, Birgir Rafn Gunnarsson, Katrín Dögg Sigurðardóttir, Þórhallur Jóhannsson and Alexander Eyjólfsson – thank you all.

Professor Rögnvaldur J. Sæmundsson, thanks for encouraging me, sharing your knowledge, and participating as a co-supervisor a master thesis with me.

The Ph.D. opportunity

The Ph.D. opportunity was possible through the assistance of many. I thank the six organizations and their representatives that participated in the research and shared their information, knowledge, and experience with me:

Blóðbankinn (The Icelandic Blood Bank - The National University Hospital in Iceland): Ína Björg Hjálmsdóttir and Sveinn Guðmundsson for their interest and willingness to share knowledge enabled me to involve master students at MIT under supervision of Professor Leveson.

Landsnet (The National Grid in Iceland): Þórður Guðmundsson, Guðmundur Ingi Ásmundsson, Íris Baldursdóttir and Guðlaug Sigurðardóttir for their interest and willingness to share knowledge enabled me to involve master students at MIT under supervision of Professor Leveson.

Landsvirkjun (The National Power Company in Iceland): Hörður Arnarson, Hildur Ríkarðsdóttir and Ármann Jónsson for their interest and willingness to share knowledge enabled me to involve master students at MIT under supervision of Professor Leveson.

Össur: Freygarður Þorsteinsson and Þorvaldur Ingvarsson for their participation.

Stiki: Huld Magnúsdóttir, Bjarni Þór Björnsson, Jianfei John Zheng, Christopher Robert Brown, Bjarni Brynjarsson, Aron Friðrik Georgsson – a big thank you for taking part in my work and for developing the STPA software tool with me and together with the STPA team at ZHAW in Switzerland.

SL lífeyrissjóður (The General Pension Fund): Sigurbjörn Sigurbjörnsson, Guðmundur Árnason, Jón Otti Jónsson and Guðmundur Stefán Steindórsson for their genuine interest in risk management and their effort in achieving ISO certifications, as the first pension fund in Iceland to do so.

Icelandic Standards and Helga Sigrún Harðardóttir, thanks for granting me access to all the ISO standards and IEC standards that were needed for this research.

Martin Rejzek and his STPA team at the ZHAW Zurich University of Applied Sciences worked with me and Stiki on developing the STPA software tool which I then used to conduct the STPA in the case studies. It was a three-year fruitful collaboration in the form of a European Eurostars funded project. It took much effort, energy, and coordination but we succeeded. The friendship that grew out of it was a big bonus. Thank you very much.

Kristrún Heimisdóttir, many thanks for our fruitful discussions, for our walks in Seltjarnarnes, for your analytic mind, rigorous thinking, and motivation.

Reykjavik University for giving me the opportunity to conduct my Ph.D. research in a friendly and encouraging environment. I am grateful for having had the opportunity to spend the entire COVID-19 period as a visiting researcher in safe surroundings while finishing writing the articles. Members of the Engineering department, the Center of Risk and Decision Analysis (CORDA) and the MPM program at Reykjavik University: Helgi Þór Ingason, Þórður Víkingur Friðgeirsson, Haukur Ingi Jónasson, Agúst Valfells and Vijay Chauhan.

The moral support

Sæmundur, my husband and colleague, you have been my unwavering supporter, co-writer, and reviewer during this Ph.D. journey. Thank you for your valuable contribution to this work, your love and support. Our sons, Björn Orri, Sigurður Finnbogi and Þorsteinn, thank you all for your love and support in my academic endeavors. My family has been the source of happiness and energy I have needed to complete this Ph.D. journey. Moms on both sides of the family, and my sisters, I thank you for always supporting and encouraging me with your best wishes.

Preface

This Ph.D. thesis is an original work by the author, Svana Helen Björnsdóttir. This doctoral work has been conducted at the School of Science and Engineering at Reykjavik University, Iceland with Páll Jensson as a main supervisor and with Nancy G. Leveson, Ioannis M Dokas, Robert Jan de Boer and Þorgeir Pálsson as co-supervisors.

Table of contents

Acknowledgements	ix
Preface	xiii
Table of contents	xv
List of Figures	xvii
List of Tables	xviii
List of Appended Publications	xix
Declaration of Contribution	1
1 Introduction	1
1.1 Background.....	1
1.2 Focus on risk analysis	3
1.3 Research context	4
1.4 Purpose, motivation, and research goals.....	5
1.4.1 Purpose.....	5
1.4.2 Motivation.....	5
1.4.3 Research objectives.....	7
1.5 Delimitations of the research	8
1.6 Thesis structure	9
2 Literature and Frame of Reference	11
2.1 Research area overview	11
2.2 Development of ISO standards and their focus on risk management.....	12
2.3 State-of-the-art risk management	12
2.4 Literature on ISO standards	13
2.5 Recent developments influencing the development of benchmarking models.....	14
2.6 Risk management in ISO standards	14
2.7 Scientific literature on risk issues in risk management systems.....	16
2.8 Scientific literature on risk and risk analysis in recent WtE projects	17
2.9 Literature review on STAMP, STPA and STECA	18
3 Research Questions and Approach	21
3.1 Research hypotheses and research questions	21
3.2 Research methodology.....	24
4 Summary of Appended Articles	31
4.1 Article A	31
4.2 Article B.....	35

4.3	Article C.....	44
4.4	Article D	52
4.5	Article E.....	60
4.6	Other publications and results from this thesis work.....	62
4.6.1	Conference presentations	62
4.6.2	Master theses.....	63
4.6.3	Development of the STPA software tool.....	64
5	Discussion	67
5.1	General risk analysis methodology.....	67
5.2	Guidance given in ISO standards on risk management	69
5.3	Alignment of ISO Standards with scientific literature on risk management	70
5.4	Risk analysis in practice	70
5.5	Development of a benchmarking model for risk management.....	71
5.6	Application of a benchmarking model for evaluation of ISO risk management systems	72
5.7	Application of STAMP and STPA	74
5.8	STAMP, STPA and STECA applied to achieve a safety and security-based design	74
5.9	Use of multiple control structures during system modeling with STAMP	76
5.10	Application of the VUCA meter.....	76
6	Conclusions and Future Work.....	77
6.1	Conclusions.....	77
6.2	Future work.....	79
	References	81
	Glossary.....	91
	Acronyms	99
	Appendices	101
	Article A The Importance of Risk Management: What is Missing in ISO Standards?.....	101
	Article B Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk	137
	Article C Aligning Stakeholders and Actors: A New Safety and Security-Based Design Approach for Major National Infrastructures	173
	Article D Modelling multiple levels of abstraction in hierarchical control structures.....	217
	Article E Can the “VUCA Meter” Augment the Traditional Project Risk Identification Process? A Case Study.....	229

List of Figures

Figure 1. Decision effectiveness during life cycle [13].....	6
Figure 2. Graphical illustration of risk management from ISO 31000:2018 [2], principles, framework and process. Figure published with permission from Icelandic Standards.....	15
Figure 3. An overview of the STPA iterative analysis process, in four steps.	18
Figure 4. An overview of research objectives, research questions and publications.	24
Figure 5. Research methodology in relation to research questions 1, 2 and 3 (Article A)...	25
Figure 6. Research methodology in relation to research questions 4,5 and 6 (Article B)...	26
Figure 7. Description of the STECA analysis process [108] (Article C).	27
Figure 8. A STAMP system model with its control structure for the WtE project.	49
Figure 9. Generic control loop of a health service.	53
Figure 10. Representation of a control structure by means of three diagrams.	55
Figure 11. The process of establishing one complete ruleset.	56
Figure 12. An abstract example of complementing views.	57
Figure 13. Two examples of the same controller showing two different levels of abstraction [123].....	58

List of Tables

Table 1. Control-theoretic analysis of textual or graphical information, based on STECA.	27
Table 2. Number of ISO certifications according to ISO surveys 2014-2019.	32
Table 3. List of ISO standards reviewed in this study.	33
Table 4. Benchmarks with correspondence to ISO 31000:2018.	37
Table 5. Organizations examined in this study.	38
Table 6. Results from the public health service (case A).	38
Table 7. Results from the public supply system (case B).	39
Table 8. Results from the construction company (case C).	40
Table 9. Results from the manufacturing company (case D).	41
Table 10. Results from the software company (case E).	42
Table 11. Results from the pension fund (case F).	43
Table 12. Overview of the risk issues found and in which organizations.	44
Table 13. List of stakeholders in the WtE project and their roles and responsibilities in the preparation and construction phase.	46
Table 14. Appearance of elements in diagram 4, 4a, and 4b in Figure 12.	57
Table 15. Appearance of the Control Structure Elements in Figure 13.	59
Table 16. The criteria for a Black Swan event adapted from [144].	62

List of Appended Publications

The following research articles, published and submitted to peer reviewed scientific Journals, form the foundation of this Ph.D. thesis:

Article A

Björnsdóttir, S.H., Jensson P., de Boer R.J., Thorsteinsson, S.E. (2021). The Importance of Risk Management: What is Missing in ISO Standards? In *Risk Analysis* (Vol. 42, No. 4, 2022). <https://onlinelibrary.wiley.com/doi/10.1111/risa.13803>

Article B

Björnsdóttir, S.H., Jensson, P., Thorsteinsson, S.E., Dokas, I.M., de Boer, R.J. (2022). Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk. In *Sustainability* 2022 (14, 4937). <https://doi.org/10.3390/su14094937>

Article C

Björnsdóttir, S.H., Jensson, P., Dokas, I.M, Thorsteinsson, S.E., Ingason H.T. (2023). Aligning Stakeholders and Actors: A New Safety and Security-Based Design Approach for Major National Infrastructures. In *Sustainability* 2023 (16, 328). <https://doi.org/10.3390/su16010328>

Article D

Rejzek M., **Björnsdóttir, S.H.**, Krauss, S.S. (2018). Modelling Multiple Levels of Abstraction in Hierarchical Control Structures. In *International Journal of Safety Science* (Vo 02, No. 01, 2018, pp. 94-103). Retrieved July 14, 2023, from: <https://en.ru.is/media/veldu-flokk/Modelling-Multiple-Levels-of-Abstraction-in--Hierarchical-Control-Structures.pdf>.

Article E

Fridgeirsson, T.V., Ingason, H.T., **Björnsdóttir, S.H.**, Gunnarsdottir, A.Y. (2021). Can the “VUCA Meter” Augment the Traditional Project Risk Identification Process? A Case Study. In *Sustainability* 2021 (13(22), 12769). <https://www.mdpi.com/2071-1050/13/22/12769>

Declaration of Contribution

The work for each paper was distributed among the authors as follows:

Article A **Björnsdóttir** planned, coordinated, and conducted the study. She also conducted the literature review and performed all analysis. She also wrote the article. Jensson, de Boer and Thorsteinsson contributed to writing, review, and editing.

Article B **Björnsdóttir** planned, coordinated, and conducted the study. She also conducted the literature review and performed all analysis. Thorsteinsson and Dokas contributed to writing, review, and editing. Jensson and de Boer contributed to the review.

Article C **Björnsdóttir** planned, coordinated, and conducted the study. She also conducted the literature review and performed all analysis. Thorsteinsson, Dokas and Ingason contributed to writing, review, and editing. Jensson contributed to the review.

Article D **Björnsdóttir** was the project manager in the work described in this conference article. Björnsdóttir and Rejzek worked together on the article. Rejzek coordinated the paper, both Björnsdóttir and Rejzek contributed to writing, review, and editing. Krauss contributed to the review.

Article E Fridgeirsson supervised the research, led the study, and arranged the article paper, He also designed the Delphi surveys, and facilitated the workshops. Ingason supervised the research and contributed to the management of the workshops, surveys, and writing. **Björnsdóttir** contributed to writing, review, and editing. Gunnarsdottir was the main researcher in the initial investigation and contributed to writing.

1 Introduction

This Ph.D. thesis describes a research in the field of risk management. There is an urgent need for new approaches to risk management, especially the analysis of risk. Industry standards are not based on risk science and risk terminology is not uniform. There is, e.g., no uniform definition for the term ‘risk’.

1.1 Background

Risk management is a term that may at first seem clear, but it has several definitions and three are specified here. The Cambridge Dictionary defines risk management as “the activity of calculating and reducing risk, so that an organization does not fail or lose money” [1]. The ISO 31000:2018 risk management guidelines defines risk management as “coordinated activities to direct and control an organization with regard to risk” [2]. The Society for Risk Analysis (SRA), a multidisciplinary, interdisciplinary, scholarly, international society that provides an open forum for all those who are interested in risk analysis, defines risk management as: “Activities to handle risk such as prevention, mitigation, adaptation or sharing. It often includes trade-offs between costs and benefits of risk reduction and choice of a level of tolerable risk” [3]. ISO 31000:2018 furthermore states that a risk management framework has the purpose “to assist the organization in integrating risk management into significant activities and functions”. The effectiveness of the framework “will depend on its interaction into the governance of the organization, including decision making” [2].

Despite the huge amount of money often used to manage risk and all the rhetoric regarding it, risk is too often treated as a compliance issue only. An issue resolved by creating rules and making sure that all employees follow them [4]. Kaplan and Mikes discuss that many such rules can of course be sensible. They can help reduce some risks, but not all. It has been criticized that rules-based risk management will neither reduce the likelihood nor the impact of many severe disasters, just as it did not prevent the collapse of many financial institutions in 2008 and the following economic crisis. This is sometimes referred to as “black swan” events; the impact of the highly improbable, after Taleb's book on the subject [5].

There is a need for a new approach to risk management. Kaplan and Mikes have introduced the idea of a new categorization of risk that allows executives to tell which risks can be managed through a rules-based model and which require alternative approaches. The big question is however: How can organizations identify and prepare for non-preventable risks that arise externally to their strategy and operations? The first step in creating an effective risk-management system is to understand the qualitative distinctions among the types of risks that organizations face. In their article, Kaplan and Mikes show that smart companies match their risk management approach to the nature of the threats they face. They discuss three risk categories. Risk events from any category can be fatal to a company's strategy and even to its survival. These three risk categories are: preventable risks, strategic risks, and external risks.

Many international standards on risk management have been published. The ISO

ISO 31000 standard deals with risk management, principles, and guidelines; and it proves useful when implementing risk management within an organization. The success of risk management will depend on the efficacy of the risk management framework providing the foundations and arrangements that will embed it throughout the organization at all levels. The risk management framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization. The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels. The risk management allows a balance to be found between taking risks and reducing them. According to ISO 31000 risk analysis is a vital part of the risk management process [2]. The identification and estimation of risk is the key to successfully evaluating and treating risk. Therefore, SRA defines risk analysis “to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level”. ISO however defines risk analysis to be one part of the risk assessment, the other two parts being risk identification and risk evaluation.

There is a big variance in how risk analysis is conducted. Specialists working in different organizations and in diverse industry sectors deal with risk analysis and risk management in different ways. It is challenging to identify and analyze risk early in the design and preparation phase of projects, instead of dealing with risk in poorly designed systems later. It is a worthy challenge to design systems and projects from the beginning with regard to risk and using the results from professionally conducted risk analysis to build safer and more secure systems.

Problems in risk analysis and risk management

As mentioned before, risk management means to coordinate activities to direct and control an organization with regard to risk. With fast-changing technology and interconnections of many kinds, the world faces new and previously unknown problems. For this reason, it is important to use reliable methods to identify risk at any time. Only if risk is identified it can be treated with mitigating controls and measures, and even then, it is important to know the residual risk.

According to Leveson, the problems in risk analysis and risk management are the following [6]:

- Increasing complexity and coupling makes it increasingly more difficult to manage risk.
- Fast changing technology increases vulnerability and therefore risk.
- New types of threats and hazards exploit vulnerabilities and increase the likelihood of a security or safety incident occurring.
- Conflicts arise between safety, security, and reliability with increased use of new technology.
- Complex technology solutions become utilities as perceived by the public, therefore tolerance for security incidents and accidents decreases.
- More complex systems mean difficulty in keeping an overview and in-depth understanding of detailed items.
- Demand for fast decision making is increasing.
- The need for prioritizing is urgent, but often difficult.

- It is difficult to keep up with changing regulatory and public views of safety and security change.

Different standards are being published as guidelines or requirements in different fields. Many of the standards do not use the same risk terminology and definition for words like 'risk' and 'threat'. This has led to confusion. The perception of risk depends on both culture and profession. Only people working in a certain field can understand the results of a risk assessment done in that field. In some fields, e.g., when assessing environmental risk and value of landscape, qualitative risk assessment methods seem to be favored. In other fields, e.g., the financial sector, quantitative methods are chosen. Quantitative data is numbers-based, countable, or measurable. Qualitative data is interpretation-based, descriptive, and relating to language. So are the quantitative research methods based on measuring and counting, while qualitative research methods are less tangible and based on interviewing and observing. Furthermore, quantitative data tells us how many, how much, or how often in calculations, while qualitative data can help us to understand why, how, or what is the reason behind certain behaviors [7], [8]. When the financial system collapsed in 2008 people learned that it is not enough to only use quantitative methods to analyze and assess risk. To obtain the experience and expertise of people who know best, qualitative methods are necessary. The question is then: When is it right to use quantitative and when qualitative methods or a combination of both? The aim of this thesis is among other things to investigate this.

1.2 Focus on risk analysis

In this thesis the emphasis is on risk analysis. Risk analysis has become ever more important as technology develops, automation increases and people's use of a variety of technical solutions grows. Risk analysis has long been a part of project management but has in recent years emerged as a specific scientific field. SRA is an example of such a scientific society [3]. This scientific community has defined several important risk concepts. There, risk analysis is broadly defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level.

Risk analysis has also become part of decision-making studies and quality management in any type of operation. The latest development of ISO standards is, e.g., largely related to risk management, and risk analysis is the basis for that. ISO standards define risk analysis in a different way than SRA, as part of risk assessment together with risk identification. Organizations that want to gain a competitive advantage, assure customers and investors of reliable procedures and quality management, many choose to obtain professional certification that requires annual verification. However, it has been a stumbling block for many who would have liked to learn about ISO standards that they have to buy the standards and pay for each update as a new standard [9], [10].

Risk analysis can be approached in different ways, and it depends on industries, cultures, and scientific fields. Risk terminology is thus different, and the use of risk terms is rarely based on scientific literature. Thus, ISO standards are issued with risk terms and definitions without reference to science or scientific literature. There, the use of risk thinking is different. Published scientific articles on this topic also state that there are large cultural differences in the assessment of risk and its severity.

As societies increasingly rely on technology and automation, many new risks and vulnerabilities are emerging. Complex systems and the interaction between people and technology means that traditional analysis techniques, e.g., Fault Tree Analysis¹ (FTA), and Failure Mode and Effects Analysis² (FMEA), are often not sufficient to detect all important hazards, threats, and risk factors. Therefore, new methods have been invented, i.a., methods based on systems theory and control theory. These methods are intended to identify and analyze better than before the causal relationship between risk factors and objects in complex sociotechnical systems. One such methodology is the Systems-Theoretic Accident Model and Processes (STAMP) accident causation model and the derived analysis techniques Systems-Theoretic Process Analysis (STPA) and Systems-Theoretic Early Concept Analysis (STECA) [6], [11], [12], [13], [14], [15]. The usefulness of these methods is specifically investigated in this thesis. They are based on an engineering approach and include those factors that can be controlled during design or operation. A method called VUCA [16], [17] is also introduced. It is intended to improve the traditional Project Management Institute (PMI) analysis method [18]. That method deals with risk events and is based more on an economic approach, on changes and instability in an environment over which the analyst has little or no control, e.g., political instability, exchange rate fluctuations, and economic instabilities.

1.3 Research context

In recent years, technology has increasingly merged with the management and organizations' activities, e.g., in the form of a variety of smart solutions and automation. At the same time, risk management has become an important part of business management and decision making. This trend can be seen from the number of ISO certifications in ISO surveys and the fact that all management system standards (MSS) in the annual ISO survey address risk management in one way or another [19].

ISO standards were initially developed as quality standards where the users of the standards define their own quality criteria. Certification audits aim at verifying that the quality is as defined by an organization, whatever it may be. Now that risk management has become an important part of all ISO management systems standards (since 2015) [20], [21], the question arises as to whether risk should be treated in a similar way. That is, if the willingness to take risk and the risk taken in ISO certified organizations is entirely the decision of the organizations' managers, and if not, how to evaluate the quality of the risk management. Quality is a unilateral decision of the organizations [22], [23], but can risk be treated as a strategic variable like quality? The risk must be identified and understood to be able to assess it and decide if and how it should be treated. Here, the application of the standards varies regarding risk and quality, and, for example, auditors face a challenge when evaluating a risk management system. Managing risk and auditing risk management systems requires knowledge of risk management, often expert knowledge on risk analysis techniques on one hand and the subject facing risk on the other hand (e.g., design, development, production, services, operations). According to the knowledge of the author of this thesis, no formal benchmarking models have been used until now as tools to evaluate the efficacy of ISO risk management systems.

¹ <https://sixsigmastudyguide.com/fault-tree-analysis/>

² <https://sixsigmastudyguide.com/failure-mode-effects-analysis-fmea/>

1.4 Purpose, motivation, and research goals

Although research within risk management has been conducted, there has been little research on the scientific base of standards, risk terminology and the efficacy of risk management processes. If guidance regarding risk management is not appropriate and if the risk analysis techniques applied fail to identify hidden risk, then ISO certifications may lead to false security by organizations managers.

1.4.1 Purpose

The main purpose of this research is to contribute to risk science. More specifically the purpose is to investigate the application of risk management standards in organizations, examine risk management processes in organizations, and the risk analysis methodologies and techniques used to identify, evaluate, and manage risk. The purpose is furthermore to:

- (a) Examine the scientific basis of standards and investigate how well aligned they are with risk science.
- (b) Investigate weaknesses in ISO standards regarding risk guidance and how consistent the risk terminology is between individual standards and with risk science.
- (c) Investigate how risk analysis is done in real ISO certified organizations, i.a., to what extent analysis methods and techniques are based on quantitative methods and qualitative methods.
- (d) Develop a benchmarking model which can be used for validation and evaluation of the foundational elements of a generic risk management system that is based on ISO standards in both a quantitative and a qualitative way
- (e) Apply the benchmarking model in real operating organizations to check how useful the model proves to be.
- (f) Investigate the application of the systems theory-based STAMP, STPA and STECA and the concept of using multiple diagrams to represent a system model.
- (g) Apply STAMP, STPA and STECA in an early stage of a major infrastructure project and investigate how useful it is in fulfilling the engineering concept of safety and security-based desing.
- (h) Investigate the analytical capabilities of the VUCA meter to identify project.

1.4.2 Motivation

The motivation for this research originates from decades of work experience in the field of risk management, i.a., from the application of ISO standards in ISO certified organizations, and the auditing of ISO management systems. This experience has revealed the importance of ISO standards, not only for businesses but also for societies, the effort in complying with them, and the fact that accredited certification activities are not a guarantee of good risk management. Over the years, certified management systems generally mature and the knowledge and experience that builds up enforces the process of improvement. When unforeseen incidents happen questions arise: Why was this risk not identified? Are there better ways to identify risks and their causal relationship? Could we have designed our systems better with regard to later managing unforeseen risk?

The application of ISO standards and ISO certifications are no assurance of the efficacy of a risk management system. The risk terminology in ISO standards is not aligned

with risk science and the ISO standards give limited guidance on how to analyze, assess, and manage risk. Experience has shown that identification and analysis of risk is an important but challenging factor in modern systems, not least during the preparation and design phase of projects and in the decision-making process. It provides the foundation for effective risk treatment, in decision making, design, development, production, construction, and operation. Conventional methods like Fault Tree Analysis (FTA) and Failure Mode and Effects Analysis (FMEA) are not adequate for risk identification and analysis in complex sociotechnical systems with many layers and interaction between individual system elements. Such systems are non-linear, and time-variant. Analysis techniques must therefore capture cross-system factors which is difficult to do with the aforementioned methods as they are based on a bottom-up approach [24], [6].

This thesis is intended to be a contribution to the development of ISO standards regarding risk management and highlight the importance of the standards' guidelines being based on scientific knowledge and that they are in accordance with the state-of-the-art in risk management. This thesis is also intended to demonstrate the importance of measurability of efficacy when it comes to assessing the quality of risk management systems and ways to do so by combining knowledge in risk management science and benchmarking theory. Benchmarking theory is theory of quality management where sustained continuous improvement is embedded in a thorough feedback mechanism. This feedback includes both internal and external benchmarks (referents) [25], [26].

Since risk analysis is one of the most critical parts of risk management, the focus is placed on the execution of risk analysis, how such an analysis is really done in ISO certified organizations and how such analysis can be improved with new methodology based on systems and control theory, such as STAMP, and the derived analysis techniques, STPA and STECA. It is a fact that early design decisions have significant impact on safety and security and can have major cost effects later in projects. The importance of integrating safety and security analysis into early project planning and systems engineering activities cannot be overemphasized. Compensating later for making poor decisions, including those affecting safety and security, can be very ineffective and costly as illustrated in Figure 1. The figure demonstrate the importance of doing risk analysis and base decision-making on the results of the analysis. If that is not done, the cost of changes at later stages will exceed cost plans and grow unforeseeable.

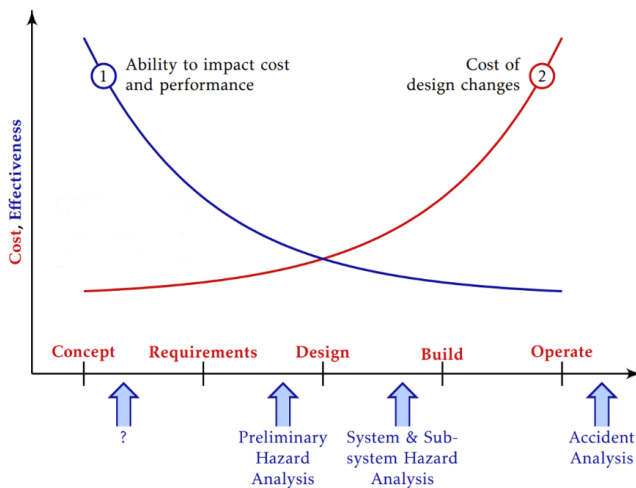


Figure 1. Decision effectiveness during life cycle [27].

1.4.3 Research objectives

Risk management is increasingly important for business. It has even become mandatory in data protection in Europe [28]. According to the annual Global Risks Reports, published by the World Economic Forum, the global economy is facing increased risks year by year in many areas and therefore the societal need for protection from harm is also increasing [29], [30], [31], [32]. This results in governmental pressure on organizations to demonstrate that they are managing risk appropriately. Standardization of risk management through compliance with industrial standards allows organizations to demonstrate their efforts in this area.

Industrial standards, especially ISO standards, are the tools organizations use to manage risk, through following their guidance and complying with their requirements. Organizations confirm their compliance with these standards through certification, which means that they heavily depend upon the quality of the ISO standards to enable them to effectively manage their risk. If the ISO management system standards and guidelines are not aligned with the scientific literature on risk, they may not be appropriate for the management of risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems.

Therefore, the research objectives in this thesis are as follows:

1. Review and compare definition of risk terms in ISO standards vs. scientific literature.
Investigate recent development of ISO standards regarding risk management. Investigate how well the ISO standards are aligned with the risk science. (Article A)
2. Conduct case studies to investigate and evaluate how risk analysis is conducted in real organizations that have proven experience with risk management through being ISO certified.
Develop and test a benchmarking model for real ISO risk management systems, to assess the efficacy of such management systems and investigate if benchmarking risk management can help identify hidden organizational risk. (Article B)
3. Investigate if the STAMP accident causation model can be used for developing a system model of the case study examples (research objective 2) to further analyze hazards, threats, and risks with the derived STPA analysis technique. Furthermore, to investigate whether STAMP/STPA can be applied to find risks that have not previously been found by the traditional methods and techniques in the case studies. This research objective could not be achieved; therefore, it was changed to research objective 5 here below. (Partly achieved in conference presentations)
4. Investigate how STAMP, combined with stakeholder theory, can be used to develop a system model of a major infrastructure project, a complex system, and thus align actors and stakeholders in such a system. Chose a project for the analysis and document the STPA and STECA analysis processes. Investigate if STAMP, STPA and STECA can be used to integrate safety and security into the project and thereby achieve the safe and secure by design engineering concept. (Article C)
5. Investigate how the representation of a STAMP system model with a hierarchical control structure can be developed as an abstract concept to capture multiple levels

of control structures in a consistent way. (Article D)

6. Investigate the analytical capabilities of the VUCA meter (Volatility, Uncertainty, Complexity, and Ambiguity) as a normative approach to identify risk in projects. (Article E)

1.5 Delimitations of the research

This research was conducted to gain knowledge about risk management in businesses, i.a., the usefulness of application of ISO standards regarding risk management, methods of risk analysis, and ways to evaluate efficacy. Part of the research was done by conducting case studies with six real-life and ISO certified organizations. The organizations were selected according to defined selection criteria, described in Article B. They operate in different industry sectors which gives breadth to the research. This means, however, that the source of the data is limited to these parties.

In the six case studies the risk management process and procedures in the organizations were investigated. Only projects that were considered successful were selected for review, because the purpose of the study and the interest of the participants was to find improvement opportunities. Successful projects refer to projects that the participants themselves considered to have been within the budget and schedule and achieved their purpose. There are several limiting factors. The main limiting factor is the number of case studies. Due to how extensive each case study is, it was not possible to carry out more than six studies in this research. Another limiting factor is the questionnaire itself, the questions may have been misinterpreted even though the questions were based on the risk management framework and risk terminology from the ISO standards which the participants should have known well, as they are all certified. One more limiting factor is the data and information that was provided, i.a., in the form of answers to the questionnaire. There is uncertainty associated with the answers, the data and information received. The purpose of the follow-up interviews was to verify data and information.

One of the main goals of the case studies was to investigate and examine to what extent the risk management systems and the analysis methods used by organizations are based on guidelines from the standards and to explore if they are aligned with risk science, despite shortcomings in the ISO standards. The results of the risk assessments from the six organizations were examined, and individual risk factors were scrutinized. This was done to investigate depth of knowledge and understanding of risk within the organizations and gather knowledge and understanding of the actual risk analysis procedure within each organization. Since this was done over a long time there may have been changes over time.

To further analyze the quality of the risk management system by the organizations in the case studies, a two-step benchmarking model was developed and tested to assess the efficacy of ISO risk management systems.

In comparison with the traditional methods that organizations use for their own risk analysis and risk assessment, the STAMP accident causation model and the derived STPA analysis technique were used. Delimited projects and systems within the case studies were selected for this analysis work. The aim was to find out if other risk factors emerged than had previously been identified, i.e., if risk factors could be found that could not be identified with traditional methods. The results of this analysis revealed sensitive information, too sensitive to publish it in scientific articles apart from what is published in Article B with consent from all participants. Since the organizations are sensitive to the publication of information about their risk that they themselves have neither identified nor had the opportunity to assess and react to, it was not feasible to publish information of that kind. It was therefore not possible to carry out

the STAMP and STPA analyses in full. Several conference lectures, however, were delivered on the topic after obtaining consent from the relevant organizations. All publications are listed in Chapter 4.

This led to a change in the scope of this thesis. To investigate the application of STAMP and the derived analysis techniques, a major national infrastructure project was chosen as subject for an analysis with STECA. No decision has yet been made regarding the project and no project owner exists. The research work is limited to information and data published in official reports, e.g., feasibility studies that have been carried out on this kind of project. Within the scope proposed for this infrastructure project, it was possible in iterative collaboration with actors and stakeholders to create a STAMP system model which then was used to conduct further analysis with STECA. The results obtained through this work are presented in Article C.

1.6 Thesis structure

The content of each chapter of this Ph.D. thesis is outlined below:

- **Chapter 1** introduces the topic, analyses the problem, purpose, and goals.
- **Chapter 2** provides a framework for this research, reviews the state-of-the-art literature on the research topic, and identifies research gaps in the area.
- **Chapter 3** describes the research approach and methodology used in this research and the research questions.
- **Chapter 4** summarizes the results and findings of each article that is appended.
- **Chapter 5** discusses the results in relation to the research goals and research questions.
- **Chapter 6** outlines the conclusions from earlier chapters and the future directions of this research.

The **Appendix** contains the full versions of the five published articles that form the basis of this Ph.D. thesis:

- Article A** The Importance of Risk Management: What is Missing in ISO Standards?
- Article B** Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk
- Article C** Aligning Stakeholders and Actors: A New Safety and Security-Based Design Approach for Major National Infrastructures
- Article D** Modelling Multiple Levels of Abstraction in Hierarchical Control Structures
- Article E** Can the “VUCA Meter” Augment the Traditional Project Risk Identification Process? A Case Study

2 Literature and Frame of Reference

This chapter presents a theoretical framework for this research, which critically assesses the state-of-the-art to identify research needs and gaps. It also provides general definitions and describes the work performed in the fields of risk management, development of international standards in risk management, risk analysis methodologies and techniques, and benchmarking regarding risk management.

2.1 Research area overview

The relevant research topics in this thesis are the following:

1. Risk management in ISO standards and in the field of international standardization.

Investigate importance of risk management for businesses and identify gaps and missing aspects regarding risk in ISO standards. Find these gaps and identify what needs to be improved and how to strengthen the basis of standards development so that standards are in line with technological development, the requirements and challenges of organizations and the complexity of today's modern sociotechnical systems. Investigate important developments regarding this within the scientific field of risk. For this purpose, a literature review is conducted with a twofold aim. First, to learn what is vital for state-of-the-art risk management. Second, to review recent literature on ISO standards themselves:

- a. Development of ISO standards and their focus on risk management,
- b. State-of-the-art risk management, and
- c. Literature on ISO standards.

2. The application of benchmarking theory in the field of risk management.

Investigation of methods for evaluating the effectiveness of risk management systems in business operations. Use of benchmarks in risk management systems that are based on ISO standards with the purpose of assessing the efficacy of the management systems and providing support and help in identifying hidden organizational risk. For this purpose, a literature review is conducted on:

- a. Recent developments influencing the development of benchmarking models,
- b. Risk management in ISO standards, and
- c. Scientific literature on risk issues in risk management systems.

3. The application of the systems-theoretic method, STAMP, and the derived analysis techniques STPA and STECA to analyze risk (including safety hazards and security threats).

Investigation and documentation of the application of STAMP, STPA and STECA in an early phase of a big and complex project. Modeling a Waste-to-Energy project with STAMP and integrating systems safety and security into the project with STPA/STECA. For this purpose, a literature review is conducted on:

- a. Scientific literature on risk and risk analysis in recent WtE projects, and
- b. Literature review on STAMP, STPA and STECA.

2.2 Development of ISO standards and their focus on risk management

Standards are important because they provide people and organizations with a level of quality, rigor, or specification that is an essential basis for the adequacy of a product or service. They are used as tools to facilitate measurement, manufacturing, commerce, and communication. ISO is an international standard-setting organization consisting of national standards bodies. ISO defines a standard as a “document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context” [33]. As the annual ISO survey shows, there is considerable use of standards in industry and public sectors today. Although ISO standards are meant to be voluntary in use, they have become increasingly important as a benchmark due to their spread and certification schemes. They are even becoming the norm in legislation and by supervisory and regulatory authorities [34], [35], [36]. The focus, and some would also say importance, of risk management in business is demonstrated by the number of organizations certified under standards addressing risk. There are basically two types of ISO standards, the Management System Standards (MSS) and the guidelines. An MSS is a standard establishing a set of interrelated or interacting elements of an organization to establish policies and objectives and to develop processes to achieve those objectives. These ISO standards, both MSS and guidelines, are hereafter referred to as ‘ISO standards’ in this Ph.D. thesis, unless otherwise specified.

2.3 State-of-the-art risk management

Applying ISO standards is a strategic investment decision. Organizations depend heavily on the guidance given in the standards to effectively manage their risk. Risk management may involve treatment of intangible aspects of assets, values, and services for which guidance or risk assessment criteria can hardly be given in standards for risk management. The user of risk management standards must be aware of this when applying those standards. For the standards to achieve their objective, it is, however, important that the standards address important risk issues and that they are in line with state-of the art risk management. In Article A sixteen examples of risk science contributions are reviewed. Some of the papers have been published by SRA, of which five were rewarded as “best paper” by SRA. Others were found through the Google Scholar search engine with search phrases on risk analysis and risk management in combination with words like “complex systems”, “nonlinear systems” “risk models”, and “sociotechnical systems”.

They describe various challenges, recent developments, and issues that are important for state-of-the-art risk management and risk analysis. The literature confirms the importance and challenges of risk analysis in complex systems. There is a call for new risk analysis methods, new risk models to capture the complex behavior and interconnection of individual time-dependent factors and interactions between people and systems. The results can be summarized to:

1. There is a need for risk models to capture (nonlinear) functions of complex and critical systems and system interactions. This is stated in scientific literature by Alderson et al. [37], Carayon et al. [38], Carreras et al. [39], Dekker et al. [40], Holovatch et al. [41], Leveson [6], [12], Rasmussen [42], and Zio [43].

2. New approaches, methods, and techniques are needed to capture and analyze risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems. This is stated in scientific literature by Alderson et al. [37], Carayon et al. [38], Carreras et al. [39], Dekker et al. [40], Holovatch et al. [41], Leveson [6], [12], Rasmussen [42], and Zio [43].
3. Risk analysis methods need to increase relevant knowledge. This is stated in scientific literature by Aven [44], Aven and Ylönen [34], Dekker et al. [40], Montibeller & Winterfeldt [45], Oughton et al. [46], Rozell [47], and Zio [43].
4. Cross-disciplinary work is needed to analyze and understand risk in sociotechnical systems. This is stated in scientific literature by Aven & Zio [48], Holovatch et al. [41], Montibeller and Winterfeldt [45], Oughton et al. [46], Rasmussen [42], and Rozell [47].
5. There is a need for a strong scientific foundation and framework for risk management suited for current and future challenges. This is stated in scientific literature by Aven [44], Aven and Ylönen [34], Aven and Zio [48], Oughton et al. [46], and Zio [43].
6. The relationship and difference between risk and resilience needs more research. This is stated in the scientific literature by Alderson et al. [37], Aven [44], Carayon et al. [38], and Zio [43].
7. Clear risk terminology is needed. This is stated in the scientific literature by Amundrud et al. [49], and Aven and Zio [48].
8. A clear ethical framework is needed as a basis for risk assessment and decision making. This is stated by Rozell [47].
9. Definitions of and the effects of not differentiating between safety and security need to be investigated and clarified. This is stated by Amundrud et al. [49].
10. Identification of leading risk indicators is needed. This is stated by Leveson [50].

2.4 Literature on ISO standards

When it comes to literature on ISO standards, it must be noted that ISO regularly updates its standards. Therefore, much of the literature on older versions of ISO standards is not relevant. In Article A a literature review was conducted on papers on “risk management in ISO standards” from 2009 and “ISO 31000 2018 risk management review” from 2018. Most of the papers reviewed in the article concern the ISO 31000:2009 version, including Aven [51], Aven and Ylönen [34], Barafort et al. [52], Leitch [53], Olechowski et al. [54], and Purdy [55]. Others the 2018 version Parviainen et al. [56], Silva Rampini et al. [57]. The changes in the standard do not affect this review. Some papers focus on risk management in information technology (IT) based on ISO standards, and integration of many ISO standards in one management system. Some authors discuss the benefits of applying ISO standards, while others are critical of the standards and their lack of scientific basis. The results of the review of literature on ISO standards can be summarized to:

1. It is important that risk terms are well-defined, clear, and uniform in all ISO standards. This is stated in scientific literature by Aven [51], Aven and Ylönen [34], Barafort et al. [52], Leitch [53], and Purdy [55].
2. Organizations heavily rely on ISO standards to manage their risk. This is stated in scientific literature by Aven and Ylönen [34], Barafort et al. [52], Purdy [55], and Silva Rampini et al. [57].
3. ISO standardization work is important because it is based on shared understanding and best practices, but that is, however, not enough for future development of the standards. This is stated by Olechowski et al. [54], and Purdy [55].

4. Collaboration and interdisciplinary work of risk specialists is needed to develop ISO standards that cover risk management. This is stated by Aven and Ylönen [34], and Silva Rampini et al. [57].
5. ISO standards are missing out on risk frameworks and risk models. This is stated by Aven [51], and Leitch [53]. Their criticism focuses on the effect of unscientific definitions of important risk terms in ISO standards and the fact that ISO 31000 defines the risk management framework as a set of components.
6. It is not enough to have market forces controlling the development of ISO standards, they must also be based on risk science. This is stated by Aven and Ylönen [34].

2.5 Recent developments influencing the development of benchmarking models

The Cambridge dictionary defines benchmarking as “the act of measuring the quality of something by comparing it with something else of an accepted standard” [58]. Benchmarking is therefore an important tool to help organizations to continuously improve the quality of their products and services. It is a popular tool in industry [59], [60], [61], [62], but it is also used in the health service to improve patient outcome, for example in surgery [63]. In this study, the quality is limited to the efficacy of the risk management system. The Cambridge dictionary defines efficacy as “the ability [...] of a method of achieving something, to produce the intended result”.

In Article B examples of benchmarking contributions are reviewed. They describe various challenges, recent developments, and issues that are important for state-of-the-art benchmarking. The literature confirms the importance and challenges of benchmarking in the assurance of quality in risk management. The results can be summarized as follows:

1. Benchmarking is important for risk management. This is stated in scientific literature by Herbst et al. [59], Kounev et al. [60], Van der Voordt et al. [62], Staiger et al. [63], Mangla et al. [64], Hoffmann et al. [65], and MacGillivray [66].
2. Benchmarking is an important tool for performance evaluation and improvement processes of organizations. This is stated in the literature by Herbst et al. [59], Kounev et al. [60], Olawumi and Chan [61], Van der Voordt et al. [62], Hartono et al. [67], Björklund [68], and Moriarty and Smallman [69].
3. In benchmarking, it may be necessary to combine quantitative and qualitative factors. This is stated in the literature by Herbst et al. [59], Kounev et al. [60], Olawumi and Chan [61], Van der Voordt et al. [62], Hartono et al. [67], Björklund [68], and Moriarty and Smallman [69].
4. A scoring system helps in defining and verifying the “quality” of risk management actions. This is stated in the literature by Olawumi and Chan [61], Hartono et al. [67], , and MacGillivray [66].
5. A benchmarking system can be applied to stimulate a genuine endeavor for perfection, rather than to judge or criticize. This is stated in the literature by Staiger et al. [63].

2.6 Risk management in ISO standards

ISO 31000 is the main ISO guideline for risk management and according to ISO the standard it “provides a common approach to managing any type of risk and is not industry or sector specific” [2]. It is intended for general guidance on risk management systems and not for certification. The first version of the standard was published in 2009 and the review in this

this work was originally based on that version. In an updated version, published in 2018, the principles of risk management have been reviewed. Greater emphasis is put on leadership by top management to ensure that risk management is integrated into all organizational activities, starting with the governance of the organization [22]. Greater emphasis is also put on the iterative nature of risk management, drawing on new experiences, knowledge, and analysis for the revision of process elements, actions, and controls at each stage of the process. According to the standard, risk management is based on the principles (described in clause 4), framework (described in clause 5), and process (described in clause 6). This is illustrated in Figure 2.

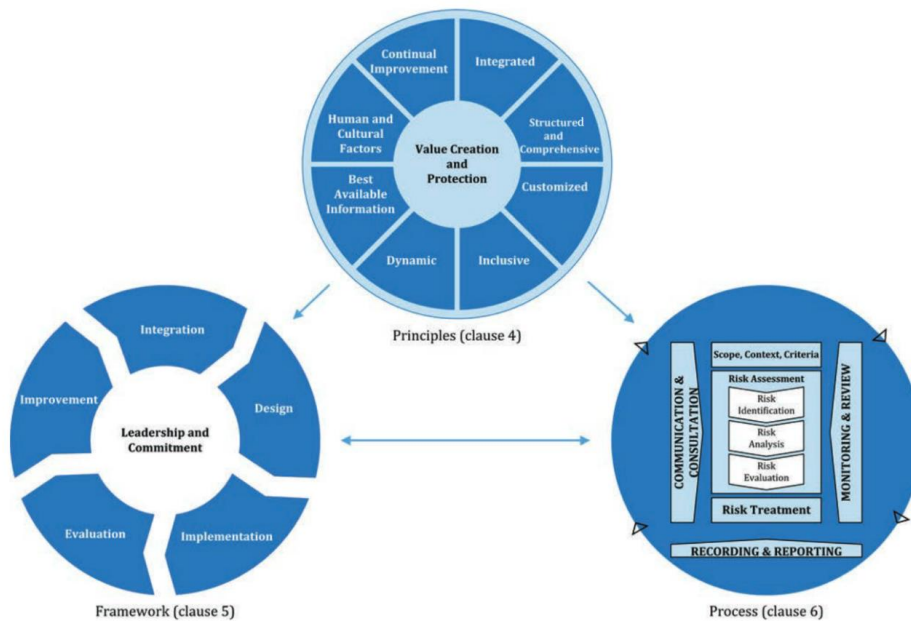


Figure 2. Graphical illustration of risk management from ISO 31000:2018 [2], principles, framework and process. Figure published with permission from Icelandic Standards.

The principles are the foundation for managing risk and should be considered when establishing the risk management framework and processes of an organization. The purpose of the risk management framework is to assist the organization in integrating risk management into activities and functions. The effectiveness of risk management depends on its integration into the governance of the organization, including decision making [70]. The components of the framework should be customized to the needs of the organization. Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all the organization's activities, including decision making. The risk management process involves the systematic application of the policies, procedures, and practices to the activities of communication and consulting, defining the scope and establishing the context, assessing, and treating risk, monitoring, reviewing, recording, and reporting risk. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope. It should reflect the organization's values, objectives, and resources, and should be consistent with policies and statements about risk management.

The ISO 31000 standard only contains guidelines, not requirements. The guidelines do not contain benchmarks, neither for risk management in general, nor individual elements of the

risk management principles, framework, or process. When auditing risk management systems that are based on ISO standards, the auditors apply the auditing standard ISO 19011 [71]. This standard is a general auditing standard, aimed at the auditing process itself and does not include benchmarks for risk management. The auditor is meant to seek written evidence of risk management, for example, the risk management process. The requirements are to be found in the ISO management system standard, such as ISO 9001 [72], ISO/IEC 27001 [73], ISO 45001 [74], ISO 13485 [35], and ISO 14001 [75].

In this study, the risk management process, as described in Figure 2, is used as a basis for benchmarking the risk management process. The requirements regarding the risk management are obtained from ISO/IEC 27001, ISO 45001, and ISO 13485, and can be summarized as follows:

1. The scope of the risk management system must be defined.
2. The risk management process must be documented.
3. Policies regarding risk management must exist and be documented.
4. Internal audits must be conducted.
5. Management review and formal review and approval for suitability and adequacy, for example, review of operational planning and control, assessments of risk, nonconformity, and the efficacy of any corrective action taken.
6. Knowledge of all legal requirements must exist.
7. Risk and root cause analysis must be conducted.
8. Risk assessment/evaluation must be conducted.
9. Criteria must be set for the management system process and risk/quality acceptance.

When a requirement needs to be “documented” in an ISO standard, it needs to be established, implemented, and maintained. The requirements of ISO 9001 and ISO 14001 are less clear regarding risk management and it is not possible to build specific benchmarks on them [76].

2.7 Scientific literature on risk issues in risk management systems

Risk management systems, as described in ISO 31000 [2], consist of risk management principles, framework, and process. According to ISO 31000, it is in the risk management process where the identification and evaluation of risk takes place, see Figure 2. The scientific basis of ISO risk management standards has been questioned in recent scientific literature [20], [48], [77], [78]. ISO standards do not reference scientific literature, only other ISO standards and sometimes risk assessment techniques and handbooks. The only bibliographic reference in ISO 31000 is IEC 31010 [79]. The IEC 31010 was first published in 2009 [80] and then updated in 2019. It is a dual logo IEC/ISO standard for supporting ISO 31000. It provides guidance on the selection and application of systematic techniques for risk assessment. Some changes have been made regarding bibliographic references in the latest version of IEC 31010:2019. In version 2009, only 11 bibliographic references were made, all to other ISO/IEC standards. In the 2019 version, there are 91 bibliographic references. Many of them are not standards but handbooks and they are categorized in the bibliography according to risk techniques with no direct reference to risk science. Therefore, the aim of the literature review is to identify risk issues that are the subject of scientific literature but not addressed in ISO standards. In this section, some examples of risk management science contributions are reviewed, as the basis for definition of benchmarks for a generic risk management process, as

described in an Article B.

The risk issues addressed in the literature can be summarized as follows and applied as benchmarks as presented:

1. Scope and outer boundaries of a risk management system [48], [81], [82], [83].
2. Interfaces (internal boundaries, departments, unclear responsibility) within a risk management system [48], [81], [82], [83].
3. Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a risk management system [48], [81].
4. Resources available to support a risk management system [78], [83].
5. Risk analysis ability to capture complex systems and business operations [20], [48], [77], [81], [82], [83].
6. Risk assessment ability to capture risk evaluation, e.g., with risk matrices [20], [77].
7. Risk criteria setting in risk assessment [20], [77].
8. Treatment of residual risk [84].

2.8 Scientific literature on risk and risk analysis in recent WtE projects

A search for published scientific articles on recent WtE projects on Google Scholar resulted in 16 articles and theses, which all were reviewed with regard to risk, identification and analysis of risk. The articles all deal with high-tech WtE incineration plants and the importance of identifying risk in such projects. What the scientific articles in this section state about risk in WtE can be summarized as follows:

1. Risk is associated with big and complex projects (i.a., megaprojects) that take several years. Circumstances can change over time and various project criteria can change [85], [86], [87], [88], [89], [90].
2. People's fear of environmental pollution causes public opposition and a bad image of waste incinerators. This creates risk and complicates WtE projects [91], [87], [92].
3. There is a risk due to inadequate communication and lack of communication with the public [92].
4. The national legislation regarding WtE involves risk. Risk is associated with inconsistencies and unclear legal provisions. Government decision making and shortcomings in legal and regulatory systems are risk factors [85], [87], [93].
5. Project financing is a risk factor and state backing is important [86], [87].
6. Establishing WtE projects as Public-Private Partnership (PPP) projects is one way to mitigate project risk, e.g., financial risk.
7. Unclear risk allocation in PPP projects creates risk [94].
8. All decision making in WtE projects must be based on results from risk analysis and risk assessment, i.e., planning, design, implementation, and operation of WtE incineration plants [94].
9. In WtE projects it is common for organizations to develop their own risk analysis methods that take into account the local environment, situation and culture [94].
10. Criteria used in risk analysis need to be carefully considered and they need to be kept under continual review [91], [95].
11. The effects on the health of people working or living in the vicinity of WtE incineration plants have not been sufficiently studied. Long-term and life cycle research needs to be done. Continuous monitoring and review of standards is important in all existing high-tech incineration plants [95].

12. Deposition of energy or heat from WtE plants influences site selection [96].
13. The choice of location and appearance of buildings is important to the public. A positive image of a high-tech incinerator can support a circular economy, improve the public's environmental awareness, and strengthen the willingness of people to take an active part in any kind of sustainability project [92], [97].
14. Technology is ever evolving. It can be assumed that the technical equipment of high-tech incinerators needs to be renewed regularly [98].
15. There is no mention of ISO standards in the scientific articles reviewed in this study, neither ISO management standards nor ISO risk management guidelines like ISO 31000:2018.
16. Delaying investment results in a loss of opportunity for selling the products from the WtE plant [99].

2.9 Literature review on STAMP, STPA and STECA

Systems-Theoretic Accident Model and Processes (STAMP) is a causality accident model for identifying system hazards and safety-related constraints necessary to ensure acceptable risk in complex systems [11], [6], [100]. STAMP was first developed by Leveson in 2004 [11] but since then widely applied and tested in many fields.

Systems-Theoretic Process Analysis (STPA) is a risk analysis technique, derived from STAMP and based on systems theory. Since introduced [6], STPA has been developed further to also analyze the security of systems with STPA-Sec [101], and with Systems-Theoretic Early Concept Analysis (STECA) [15], [102], [27]. Scientific studies have been conducted on the use of STPA in many areas, e.g., aviation, spacecraft, healthcare, railroads, automobiles, military, nuclear power plants, oil, and gas (petrochemicals) and energy. Interdisciplinary studies have also been conducted on, e.g., human factors and safety, integration of safety into systems engineering processes, identifying leading indicators of increasing risk, application of standards and certification, the role of culture, social, and legal systems on safety and security. To the knowledge of the author, STAMP/STPA/STECA have not been applied in WtE projects and no scientific articles or reports on STAMP/STPA/STECA in such projects were found on Google Scholar.

According to the STPA handbook [13], the basic STPA is conducted in four main steps: (1) define purpose of the analysis; (2) model the control structure in accordance with STAMP; (3) identify unsafe control actions; (4) identify loss scenarios. Figure 3 gives an overview of the STPA iterative analysis process.

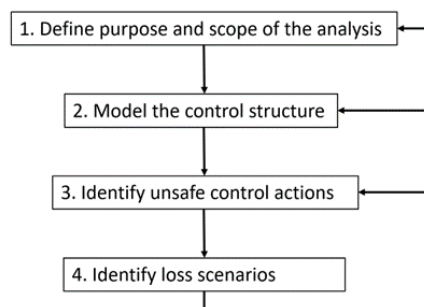


Figure 3. An overview of the STPA iterative analysis process, in four steps.

STPA is still being developed as a technique in many parts of the world, especially steps 3 and 4. This is described in many recent scientific articles, either as a theoretical analysis of the technique or as case study articles on actual application examples. In this review the focus is on practical application of the STAMP/STPA technique in an early-stage project concept. Therefore STECA, as an early concept analysis variant of STAMP/STPA, is an interesting technique to test and confirm the feasibility of the WtE project. In STECA, the emphasis is on preparing a model to be used for safety/security hazard analysis during the preliminary inspection of the project. Since the WtE project is only at the discussion stage and no decision has been taken of any kind, it is neither possible to make scenarios about “unsafe control action” nor “identify loss scenarios”. It is only possible to take the first two STPA steps out of four, i.e., to define the scope and develop the model.

STECA consists of two basic steps. The first step involves recursively applying control-theoretic concepts using guide words, heuristics, and feedback control criteria to parse the existing concept report and review it with regard to statutory and regulatory requirements. Also, the main results regarding the project, e.g., waste amount and possible location, are used as Concept of Operations (ConOps), resulting in the development of a control structure of the model of the concept. With STECA it should be possible to determine the hierarchical control structure but, in this case, it is not relevant since laws and regulations determine the hierarchical structure for the most part. The second step in STECA, the analysis, consists of examining the resulting model with the explicit goals of identifying hazardous/threat scenarios, information gaps, inconsistencies, and potential tradeoffs and alternatives. The analysis aims at identifying incompleteness or gaps in the control structure, ensures that all safety/security-related responsibilities are accounted for, and identifying sources of uncoordinated or inconsistent control [15], [102], that is to:

1. Identify incompleteness or gaps in the control structure.
2. Ensure that all safety-related responsibilities are accounted for.
3. Identify sources of uncoordinated or inconsistent control.

The lessons learned from reviewing articles [103], [104], [105], [106], [107], [108], [109] on the application of STAMP, STPA and STECA can be summarized to:

1. The STAMP, STPA and STECA techniques are helpful in the development of system and project modeling, especially in complex systems and projects.
2. The STAMP and STECA techniques are helpful in early concept analysis, building the system model.
3. The STAMP and STPA techniques are helpful in further design, especially when analyzing complex systems and projects.
4. The STPA handbook does not always provide the necessary guidance and level of support when developing a control structure of a new design.
5. STAMP and STPA are often supplementary to other risk analysis techniques, e.g., FTA, FMEA, Hazard and Operability (HAZOP), UPPAAL technique, named after Uppsala University (UPP) in Sweden and Aalborg University (AAL) in Denmark, and Functional Resonance Analysis Method (FRAM).

3 Research Questions and Approach

The overall aim of this Ph.D. thesis is to contribute to risk management science by investigating the efficacy of risk management, especially risk analysis which is an important part of risk management if risk is to be treated in a manageable and appropriate manner. The research topic is manifold, e.g.:

- The process of risk management.
- The importance and usefulness of international standards and certification in business when it comes to risk management.
- Risk terminology.
- Scientific research in the field of risk analysis and to what extent international standards are based on scientific literature.
- Models to benchmark risk management.
- The need for new methods to identify risk due to increasing complexity of systems, changes in technology and human society.

This chapter presents the research hypotheses that are put forward as statements that introduce research questions and propose expected results. The chapter also describes the research approach and methodology.

3.1 Research hypotheses and research questions

Based on the research focus of this thesis, the following research questions have been formulated with the aim of answering them throughout the thesis.

Research question 1.

To what extent is it possible to formulate a general risk analysis methodology that can be used in many different disciplines?

The aim here is to gain domain-specific knowledge about risk management and the needs organizations have regarding identifying, analyzing, evaluating, and treating risk. The research question also aims to elaborate on what kind of risk analysis methodology would be appropriate for the management of risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems.

Research question 2.

What guidance is given in ISO standards on risk management, especially for the critical step of risk analysis?

The aim here is to gain knowledge and contribute to the further development of the area of risk analysis and risk management in the International Organization for Standardization (ISO) standards by strengthening their scientific basis. Industrial standards, especially ISO standards, are the tools organizations use to manage their risk, through following their guidance and complying with their requirements. Organizations confirm

their compliance with these standards through certification, which means that they heavily depend upon the quality of the ISO standards to enable them to effectively manage their risk. The aim is therefore to investigate what guidance is given on key elements of risk management in all ISO MSS included in the annual ISO survey and the guidelines they refer to regarding risk, altogether eighteen ISO standards. By investigating the development over 8 years it is possible to evaluate the trend regarding the emphasis on risk in the standards, their spread and development in the number of certificates.

Research question 3.

How well-aligned are ISO standards with the scientific literature and state-of-the-art thinking on risk?

This research question is interrelated with research question 2 and focuses on the substance of the guidance based on the outcome of the previous research question. The aim is to evaluate how well ISO standards are aligned with state-of-the-art risk management literature, review the risk terminology in the standards, and the consistency between individual standards regarding definitions of risk terms. The aim is furthermore to explore if the standards reflect collaboration with academic organizations and experts in risk science. If they do not, the standards may not be appropriate for the management of risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems.

Research question 4.

How is risk analysis conducted in real ISO certified organizations?

The aim here is through case studies to gain knowledge of the analysis techniques ISO certified organizations use.

Research question 5.

Can a general benchmarking model for risk management be developed to evaluate the quality of a risk management process that is based on ISO MSS?

The aim here is to investigate if risk science knowledge combined with benchmarking theory can be used to benchmark ISO risk management systems. In the ISO 31000 guidelines all key elements of a risk management system are defined. The aim is to investigate if special benchmarks can be defined, based on ISO 31000, to provide rigor when assessing and evaluating the efficacy of an ISO risk management system.

Research question 6.

How useful is a benchmarking model for risk management in terms of finding hidden risk issues and improvement opportunities?

The aim here is to conduct case studies to test the outcome of research question 5 by applying the benchmarking model to real ISO certified organizations and investigate if risk issues and risk factors can be found that had not previously been identified.

Research question 7.

Can STAMP and STPA analysis technique be applied to identify hazards, threats and risks that have not been previously found?

The aim here is to apply STAMP and STPA in case studies in real ISO certified

organizations and investigate if risk issues and risk factors can be found that had not previously been identified with traditional risk analysis techniques.

Research question 8.

Can the STAMP, STPA and STECA analysis techniques be applied to create a system model that can then be used to confirm a major national infrastructure concept? Can the model and the analysis techniques furthermore be used to identify and analyze project risk, and define requirements regarding risk mitigation from the early phase of the project and in that way fulfill the requirements of the engineering concept SbD?

The aim here is to investigate the usefulness of modeling a project with STAMP and conduct risk analysis on the model before any decision has been made to verify the concept and identify and analyze risk at the beginning to support decision making and project design. The aim is furthermore to investigate if the risk analysis techniques can help identifying the most important risk factors to deal with at any given time and support analysts in making decisions at a given time. Concurrently, the purpose is to document in detail the development of the model and the analysis process.

Research question 9.

Can the concept of control structures in STAMP be developed to capture the use of multiple diagrams to represent one model?

The aim here is to investigate the concept of multiple diagrams representing one and the same STAMP system model. Usually, the representation of a STAMP model is restricted to a single diagram. This modeling work typically starts at a rather abstract level but is then refined during the modeling or at later stages in the analysis process. Usually, no differentiation is made between the control structure model and its representation as a diagram. The aim is furthermore to analyze the rulesets needed to represent one model using multiple diagrams. In this regard it is necessary also to consider consistency issues, e.g., that the control structure representations are consistent with the model and with each other, and how to ensure the completeness of the STPA analysis made based on the model.

Research question 10.

Can the VUCA meter augment the traditional project risk identification process?

The aim here is to investigate the analytical capabilities of the VUCA meter normative approach to identify risk in projects that includes complexity, uncertainty, volatility, and ambiguity.

Figure 4 depicts the connections between the research objectives, research questions and publications. All research objectives were achieved except research objective 3, which was only partly achieved through conference presentations.

Research objectives	Research questions	Publications
1. - Risk in ISO standards vs. scientific literature - Recent development of ISO standards w.r.t. risk management - Alignment of ISO standards with scientific literature	Q1: Can a general risk analysis methodology be formulated? Q2: What guidance is given on risk management and risk analysis in ISO standards? Q3: How well are ISO standards aligned with scientific literature on risk?	Article A
2. - Risk analysis in real ISO certified organizations - Benchmarking ISO risk management systems	Q4: How is risk analysis conducted in real ISO certified organizations? Q5: Can a general benchmarking model be developed to evaluate risk management based on ISO standards? Q6: How useful is the benchmarking model in terms of finding hidden risk issues and improvement opportunities?	Article B
3. Capability of STAMP/STPA to identify risk that previously could not be found	Q7: Can STAMP/STPA be applied to find risks that have not previously been found with traditional risk analysis techniques?	Partly achieved in conference presentations
4. Application of STAMP/STPA/STECA to achieve the Sbd concept in an early concept phase of a major infrastructure project	Q8: Can STAMP/STPA/STECA be used to confirm the project concept and achieve the Sbd engineering concept?	Article C
5. STAMP hierarchical control structures in multiple levels	Q9: Can the concept of control structures in STAMP be developed to capture the use of multiple diagrams to represent one model?	Article D
6. Analytical capabilities of the VUCA meter to identify project risk	Q10: Can the “VUCA meter” augment the traditional project risk identification process?	Article E

Figure 4. An overview of research objectives, research questions and publications.

3.2 Research methodology

This research aims, through literature review, analysis and comparison of current methodology used for risk analysis in different fields, to seek a general methodology for conducting risk analysis in every field. The research methodology includes data gathering and literature overview. The literature review is conducted to delimit the scope of the theses, identify the main methodologies and research techniques that have been used and gain methodological insights and new perspectives in risk analysis. The goal of the literature review is also to identify recommendations for further research. Literature review includes problem formulation and delimiting the research problem. The data collection process continues until the point of saturation is reached. Data evaluation includes defining literature scoring rubric.

The main research question is if a general risk analysis methodology can be formulated that can be used in many fields. To approach this research question, 18 ISO standards (listed in Table 2 and Table 3) were reviewed with regard to business needs for risk management and risk issues found, as presented in Article A: (1) context of business needs; (2) description of risk; (3) description of risk models; (4) description of risk analysis; (5) description of risk in complex sociotechnical systems; (6) alignment with scientific literature. Figure 5 describes the research methodology and its individual steps in a schematic way. The figure reflects research questions 1, 2 and 3. It also reflects the structure of Article A.

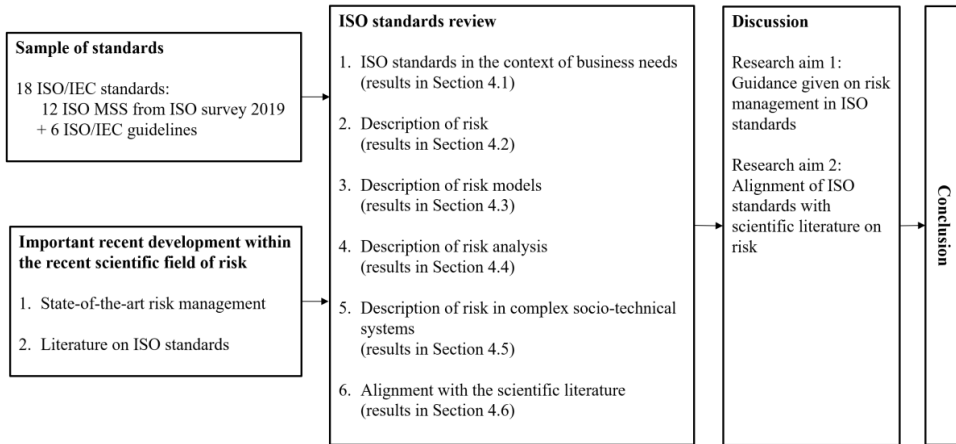


Figure 5. Research methodology in relation to research questions 1, 2 and 3 (Article A).

The second part of the research included developing a benchmarking model and testing it through case studies. After developing the benchmarking model described in Article B, the research proceeded in the following five steps: (1) setting selection criteria for participants in the case studies; (2) selection of business sectors and organizations; (3) conducting of a risk management questionnaire (for the quantitative part of the research) based on the benchmarking model in Step 1; (4) follow-up interviews (for the qualitative part of the research); (5) evaluation of the risk management process applying the benchmark model developed in Step 2. Figure 6 gives an overview of this part of the research process. It describes the research methodology and its individual steps, also reflecting the structure of Article B. The six case studies were also conducted to investigate what risk analysis methodologies and techniques are used in different fields. The fields investigated are (a) a public health service, (b) a public supply system, (c) a construction work, (d) manufacturing of medical devices, (e) software development, and (f) pension fund investments. Six organizations, fulfilling these the research criteria mentioned above. Five of them already had accredited certification to one or more ISO standards when the case study started in 2014, one was in the implementing phase and received accredited certification during the time of the study, end of 2018. Written contracts were made with all organizations to ensure information security according to the requirements of ISO/IEC 27001:2013 [3] throughout and after the case study process. A contact person with expertise in risk was nominated in every organization, responsible for the delivery of information, orally and written. After signing contracts and confidentiality agreements, meetings were held with the contact persons and their teams to inform them, explain the aim of the research, answer questions, and clarify expectations on both sides.

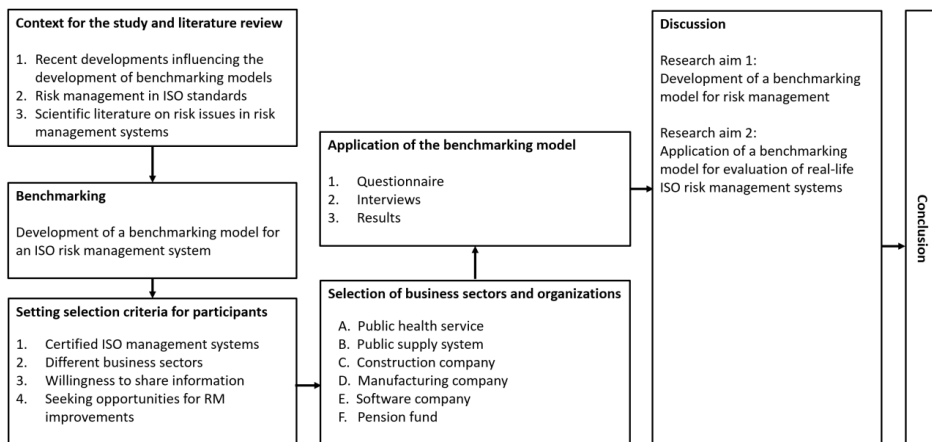


Figure 6. Research methodology in relation to research questions 4,5 and 6 (Article B).

The third part of the research was a study described in Article C on the application of the systems theory-based STAMP, STPA and STECA technique together with the derived hazard, threat, and risk analysis techniques STPA and STECA. A system model was created with STAMP showing stakeholders and their communication. The first steps of STPA were taken by identifying major possible accident and accidents and system-level hazards and threats that can lead to those accidents and losses. To be able to conduct a full STPA the system must, however, be defined and known. Here, STECA proves to be a useful technique to analyze the necessary system elements and the corresponding communication, both actions and feedback. In this case STECA together with STPA were used to help define the WtE project scope, with the help of stakeholder theory identifying actors and stakeholders, defining stakeholders' responsibilities, their connection and necessary communication with each other. This was done to identify the prime risk factors in the early concept phase.

This research proceeded in the following ten steps:

1. Definition of the scope of the WtE project.
2. Review of all relevant Icelandic law and regulations on waste management, environmental issues, local government issues, health issues, building regulations, and the European directive on environmental issues in relation to role and responsibility in a WtE project.
3. Definition of stakeholders, based on step 1.
4. Role and responsibilities of all stakeholders from step 2 based on requirements in laws and regulation reviewed in step 1.
5. First draft of the control structure of the WtE system, representing stakeholders and their communication, based on stakeholder analysis in steps 1 and 2. A graph was made of the communication required between stakeholders according to laws and regulations, both feedback and control actions resulting from step 3.
6. Identification of control actions as subsystems where there might be a reason to make special models.
7. STAMP system model reviewed by stakeholders and actors in different fields. Validation sought for every part of the STAMP system model, i.e., stakeholders, responsibilities, feedback needed, control actions needed, and sub processes within the model. Detailed description can be found in Article C.
8. First two steps taken in STPA based on the validated STAMP system model. Stakeholders and actors, experts on individual project aspects from step 7 were asked

which losses/accidents and system-level hazards/threats may not occur in the project at all, and furthermore which hazards/threats they believe could cause such losses/accidents. These two STPA steps further confirm the STAMP model and point to important aspects of the project discussed in the results section.

9. Review of the project scope.
10. Refinement of the STAMP system model and description of control actions. Control action analysis made regarding whether an action is: (a) requirement, (b) output, (c) one time action, or (d) continuous action.

In this part of the research the STECA process was followed as shown in Figure 4.

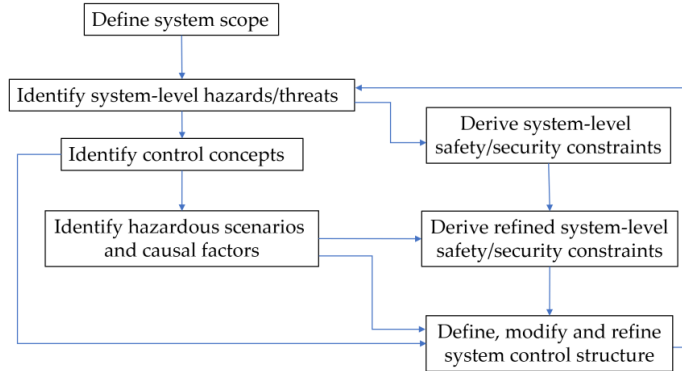


Figure 7. Description of the STECA analysis process [110] (Article C).

The research methodology also included verification of the system model as described in Article C. If the STECA process is continued, then the analysis continues with the modeling and analyzes of the hierarchical safety/security control structure. In this study hierarchical control is not critical. It is, at this point, defined by law and regulation. The modeling analysis is focused on: (a) identification of stakeholder, (b) responsibility of stakeholder, (b) feedback needed from stakeholder, (c) action required from stakeholder, and (d) description of action. Table 2 shows the control-theoretic analysis of textual or graphical information from the feasibility study and from document review, based on STECA.

Table 1. Control-theoretic analysis of textual or graphical information, based on STECA.

Name of model item/element	Definition
Stakeholder (matches “source/subject” in STECA)	A legal entity that is required in the project
Responsibility (matches “role” in STECA)	Legal responsibility as stated in law – or necessary role for some reason, that should be documented.
Feedback needed (from which stakeholder(s)?) (matches “behavior type” of the nature “action” in STECA)	For a given responsibility/role, which type(s) of feedback behavior is required or exhibited?
Action required (towards which stakeholder(s)?) (matches “behavior type” of the nature “action” in STECA)	Description of control action (CA): (a) is it a clear control action, (b) is it a requirement, (c) is it a simple output?

No further STPA steps could be taken at this point. For that to happen, a decision must be made on several important factors, e.g., who will participate in the project and the project owner setup (owner structure), what location will be chosen for the incineration plant, and what is the time frame of the project, i.e., when should the project start and when should it end.

In the fourth part of this research an opportunity arose to collaborate with ZHAW in Switzerland and explore the STAMP model development and investigating the possibility of breaking the STAMP system model down into specific system models. The research work was guided by ZHAW, but the software development project itself was managed as a part of this thesis work. It started with a STAMP/STPA workshop where a team of 7 people took part. The project lasted for 3 years, during which regular project meetings were held every 1-4 weeks to discuss and review individual aspects of the project. A detailed description of the STAMP modeling research is described in Article D.

The final part of this research consisted of investigating whether the VUCA meter augments the traditional project risk identification process. A detailed description of the research methodology can be found in Article E. Two workshops were lined up for the study. The main goal of the workshops was to apply and compare two different approaches for identification of risk factors in the selected project: firstly, a conventional risk identification as presented by PMI, where the main risk factors are identified on the basis on given focus questions and then rated on a scale for the likelihood of them occurring and the impact they would have; secondly, the VUCA risk identification method, where the main risk factors are identified based on five focus questions for each part of the term VUCA, 20 questions in total. In this case, the questions were composed based on the VUCA meter [16].

The questionnaire for the conventional risk identification was based on the traditional method presented in the PMI Standard for Risk Management in Portfolios, Programs, and Projects [18]. It was divided into four focus questions and was answered by listing factors that could be risky for the project related to each focus question. The focus questions were: (a) What risk events can impose operational risk? (b) What risk events can impose financial risk? (c) What risk events can impose legal and regulatory risk? and (d) What risk events can impose strategic risk? Each risk factor was given value for the likelihood of occurring and for the impact if it occurs. The values given for the likelihood and the impact are in the range of 1 to 5. The numbers indicate the following: (1) very low, (2) low, (3) medium, (4) high, and (5) very high.

The questionnaire for the VUCA risk identification was divided into four categories. Each category represented one of the four concepts VUCA with five focus questions:

1. Volatility: (a) What complexity factors could lead to the need for many interfaces with other technologies, projects, or operations? (b) What volatility elements could lead to the need for more resources than expected? (c) What, from the perspective of volatility, could cause the project to take longer than planned? (d) What volatility factors could impact solid contract situation throughout the project timeline? (e) What volatility factors could cause the need for major changes in the objectives of the project?
2. Uncertainty: (a) What uncertainty factors could lead to the need for more information about technology components of the project? (b) What uncertainty factors could lead to the need for many stakeholders from different time zones? (c) What could cause the access to information to be limited due to uncertainty? (d)

- What uncertainty factors could impact well defined and approved scope? (e) What uncertainty factors could impact well-defined risk management?
3. Complexity: (a) What could lead to a complex political environment with many regulations to follow? (b) What complexity factors could lead to the need for many subcontractors, organizational departments, and cultural differences? (c) What complexity factors could lead to the need for many interfaces with other technologies, projects, or operations? (d) What are the factors of complexity making this a unique project not done before? (e) What complexity factors could make the decision-making not be straightforward?
 4. Ambiguity: (a) What could cause the deliverables to not be as defined in the beginning due to ambiguity? (b) What ambiguity factors could cause the connections between tasks to become unclear? (c) What could lead to unexpected and unforeseen risk factors in an ambiguity environment? What could cause hidden agenda due to ambiguity? (e) What could lead to the need for unexpected/unknown stakeholders due to ambiguity? Brainstorming techniques were applied in both workshops and the individuals in the workgroups carefully facilitated. Pictures from the workshops can be found in Article E.

4 Summary of Appended Articles

The five appended articles are parts of a research with the overall aim to contribute to the further development of the area of risk analysis and risk management in ISO standards by strengthening its scientific basis.

Article A focuses on eighteen ISO standards and examines what guidance is given on key elements of risk management and how well ISO standards are aligned with state-of-the-art risk management literature.

Article B focuses on benchmarking in risk management. The article introduces a two-step benchmarking model to assess the efficacy of ISO risk management systems. It furthermore aims at verifying its usefulness in terms of finding hidden risk issues and improvement opportunities.

Article C focuses on a systems-theoretic methodology to meet the requirements of a major national infrastructure for safety and security-based design by enhancing the alignment of stakeholders and actors in the project.

Article D focuses on the process of STAMP and STPA, levels of abstraction, rulesets, and constraints allowing complementing views.

Article E focuses on the application of the VUCA Meter as an augment to the traditional project risk identification process.

4.1 Article A

The **aim** of Article A was twofold: (1) to investigate and evaluate guidance given in ISO standards on risk management, especially for the critical step of risk analysis; and (2) to investigate how well aligned the standards are with the scientific literature and state-of-the-art thinking on risk.

The **challenge** was to review 18 ISO and IEC standards and to collect statistics on ISO certifications according to ISO surveys for the period 2014 – 2019 (results are published the year after). Many of the standards changed during the period of the research. This meant monitoring all changes in the standards during that time and interpreting the changes with regard to the most recent scientific literature. It was a challenge to achieve and maintain an overview of the research topic while working on the research, which took eight years (2013-2021).

The **key contribution** of Article A consists of an overview of the development of international standards in recent years and the confirmation of the growing importance of risk management and risk analysis in all management systems. The article confirms the increasing importance of risk management for business. However, the article also shows a lack of guidance on doing risk analysis in the standards examined. The article shows that the ISO management system standards and guidelines are not aligned with the scientific literature on

risk and are not appropriate for the management of risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems.

The **piece of insight** generated from Article A was multifarious. In recent years, technology has increasingly merged with the management and organizations' activities, e.g., in the form of a variety of smart solutions and automation. At the same time, risk management has become an important part of business management and decision making. This trend can be seen from the number of ISO certifications in ISO surveys shown in Table 2 for the period 2014-2019. The article gives insight into the spread of ISO standards and the number of organizations around the world that see reasons to obtain accredited certification in their operations. All management system standards (MSS) in the ISO survey 2019 address risk management in one way or another, which was not the case in 2014.

The overview of annual ISO surveys in Table 2 show the growth of certifications globally [19]. ISO considers it only feasible to include the most used standards in the survey. Certification bodies are requested to fill out a questionnaire on the number of certificates per country and industry sectors, by standards. The survey counts the number of certificates issued by certification bodies that members of the International Accreditation Forum (IAF) have accredited [111].

Table 2. Number of ISO certifications according to ISO surveys 2014-2019.

ISO Mgmt. System Standard	Title	Number of Certifications					
		2019	2018	2017	2016	2015	2014
ISO 9001:2015 ^(1,2)	Quality management systems — Requirements	883.521	878.664	1.058.504	1.105.937	1.034.180	1.036.321
ISO 14001:2015 ^(1,2)	Environmental management systems — Requirements with guidance for use	312.580	307.059	362.610	346.147	319.496	296.736
ISO 45001:2018 ^(1,2)	Occupational health and safety management systems — Requirements with guidance for use	38.654	11.952				
ISO/IEC 27001:2013 ^(1,2)	Information technology — Security techniques — Information security management systems — Requirements	36.362	31.910	39.501	33.290	27.536	23.005
ISO 22000:2005&2018 ⁽¹⁾	Food safety management systems — Requirements for any organization in the food chain	33.502	32.120	32.722	32.139	32.061	27.690
ISO 13485:2003&2016 ⁽¹⁾	Medical devices — Quality management systems — Requirements for regulatory purposes	23.045	19.472	31.520	29.585	26.255	26.280
ISO 50001:2011&2018 ⁽¹⁾	Energy management systems — Requirements with guidance for use	18.227	18.059	21.501	20.216	11.985	6.765
ISO/IEC 20000-1:2011&2018 ^(1,2)	Information technology — Service management — Part 1: Service management system requirements	6.047	5.308	5.005	4.537	2.778	
ISO 28000:2007 ⁽¹⁾	Specification for security management systems for the supply chain	1.874	617	494	356		
ISO 22301:2019 ^(1,2)	Societal security — Business continuity management systems — Requirements	1.693	1.506	4.281	3.853	3.133	1.757
ISO 37001:2016 ^(1,2)	Anti-bribery management systems	872	389				
ISO 39001:2012 ^(1,2)	Road traffic safety (RTS) management systems — Requirements with guidance for use	864	547	620	478		
ISO/TS 16949:2009 ⁽¹⁾ -- NOT included in ISO survey since 2016	Quality management systems — Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations				67.358	62.944	57.950
Total number of certifications:		1.357.241	1.307.603	1.556.758	1.576.538	1.457.424	1.418.554
Change year over year:		3.8%	-16.0%	-1.3%	8.2%	2.7%	

(1) refers to risk management; (2) refers to ISO 31000.

The overview of annual ISO surveys in Table 2 show the growth of certifications globally [19]. ISO considers it only feasible to include the most used standards in the survey. Certification bodies are requested to fill out a questionnaire on the number of certificates per country and industry sectors, by standards. The survey counts the number of certificates issued by certification bodies that members of the International Accreditation Forum (IAF) have accredited [111]. The number of standards included in the annual ISO survey has increased in

past years, and ISO survey 2019 (published in September 2020) included twelve ISO/IEC³ MSS [19]. Eight out of twelve refer to six different ISO/IEC risk management guidelines. These 18 MSS standards and guidelines (referred to as ISO standards), create the data source for this study, see Table 3. In this article these standards are examined regarding consistency in risk terms, guidance (description), and scientific foundation.

Table 3. List of ISO standards reviewed in this study.

Type of Standard	Name of Standard	Purpose of Standard
MSS	ISO 9001	Quality management
MSS	ISO 14001	Environmental management
MSS	ISO 45001	Occupational health and safety
MSS	ISO/IEC 27001	Information security
MSS	ISO 22000	Food safety
MSS	ISO 13485	Medical devices (for regulatory purposes)
MSS	ISO 50001	Energy management
MSS	ISO/IEC 20000-1	Information technology service
MSS	ISO 28000	Supply chain security
MSS	ISO 22301	Societal security and business continuity
MSS	ISO 37001	Anti-bribery security
MSS	ISO 39001	Road traffic safety
Guidelines	ISO 31000	Risk management (general)
Guidelines	IEC 31010	Risk management (risk assessment)
Guidelines	ISO Guide 73	Risk management (vocabulary)
Guidelines	ISO/IEC 27005	Risk management (information security)
Guidelines	ISO 14971	Risk management (medical devices)
Guidelines	IEC 62366-1	Risk management (usability engineering & medical devices)

The 18 ISO standards reviewed in the article are listed with full names below. They were examined with regard to consistency in risk terms, guidance (description), and scientific foundation:

1. ISO 9001:2015, Quality management systems - Requirements [72]. This is one of the first standards ISO published. Risk was included as an explicit concept in the standard for the first time in 2015. The standard states that it “specifies requirements for the organization to understand its context and determine risk as a basis for planning. This represents the application of risk-based thinking to planning and implementing quality management system processes and will assist in determining the extent of documented information”.
2. ISO 14001:2015, Environmental management systems - Requirements with guidance for use [75]. This standard also adopted the risk concept in 2015, like ISO 9001.
3. ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements [73].
4. ISO 22000:2018, Food safety management systems - Requirements for any organization in the food chain [112].

³ IEC stands for the International Electrotechnical Commission, an international standards organization that publishes international standards for all electrical, electronic and related technologies – collectively known as “electrotechnology”.

5. ISO 45001:2018, Occupational health and safety management systems - Requirements with guidance for use [74].
6. ISO 13485:2016, Medical devices - Quality management systems - Requirements for regulatory purposes [35].
7. ISO 50001:2018, Energy management systems - Requirements with guidance for use [113].
8. ISO 22301: 2019, Societal security - Business continuity management systems - Requirements [114].
9. ISO/IEC 20000-1:2018, Information technology - Service management - Part 1: Service management system requirements [115].
10. ISO 28000:2007, Specification for security management systems for the supply chain [116].
11. ISO 37001:2016, Anti-bribery management systems [117].
12. ISO 39001:2012, Road traffic safety (RTS) management systems - Requirements with guidance for use [118].
13. ISO 31000:2018&2009, Risk management - Principles and guidelines [2]. First published in 2009, updated 2018. General principles and guidelines on risk management that describe a generic approach for managing any form of risk in a systematic, transparent, and credible manner. To be applied within any scope and context. The only bibliographic reference in ISO 31000 is IEC 31010.
14. IEC 31010:2019&2009, Risk management - Risk assessment techniques [79]. First published in 2009, updated 2019. A dual logo IEC/ISO standard for supporting ISO 31000. It provides guidance on selection and application of systematic techniques for risk assessment. Some changes have been made regarding bibliographic references in the latest version of IEC 31010:2019. In version 2009 only 11 bibliographic references were made, all to other ISO/IEC standards. In the 2019 version, the bibliographic references are 91. Many of them are not standards but handbooks and they are categorized in the bibliography according to risk techniques with no direct reference to risk science.
15. ISO Guide 73:2009 [119] provides a basic risk management vocabulary, for common understanding on risk management concepts and terms in other ISO standards and across different applications. The introduction to the guide states that its aim is “to provide basic vocabulary to develop common understanding of risk management concepts and terms among organizations and functions, and across different applications and types”. Its aim is furthermore “to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.”
16. ISO/IEC 27005:2018 [120] provides guidelines for information security risk management. The standard supports the general concepts specified in the ISO/IEC 27001 standard and is designed to assist in satisfactory implementation of information security, based on a risk management approach.
17. ISO 14971:2019 [36] is for applying risk management in manufacturing of medical devices. The standard specifies a process for manufacturers to identify the hazards associated with medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls. The requirements are meant to apply to all life-cycle stages of a medical device.

18. IEC 62366-1:2015 [121] is developed jointly by IEC and ISO and provides guidelines for usability engineering to medical device. It specifies a process for manufacturers to analyze, specify, develop, and evaluate the usability of medical devices as related to safety. It refers to the human factors engineering process that permits the manufacturer to assess and mitigate risks associated with normal use, i.e., correct use and use errors. It can be used to identify risks but does not cover abnormal usage.

Table 2 also provides insight into the spread of standards and the number of organizations around the world that see reason to obtain professional certification in their operations. The article furthermore gives insight into the increasing focus on risk management in most business sectors and in ISO standards since 2014. The article also gives insight into the diversity in the risk terminology across ISO standards. There is little mention of risk models in the standards and there is a lack of guidance on doing risk analysis in ISO standards. There is also little mention of risk in complex sociotechnical systems in ISO standards, despite increased risk in such systems and their growing importance. Last, but not least, the article gives insight into the lack of alignment with the scientific literature on risk management in the ISO standards.

4.2 Article B

The **aim** of Article B was twofold. Firstly, to develop a benchmarking model for risk management based on scientific literature and ISO standards to assess the efficacy of real risk management systems and see whether hidden risk can still be identified through ISO standard risk management systems and the risk assessment process used by operating organizations. The article introduces a two-step benchmarking model to assess the efficacy of ISO risk management systems. Secondly, the aim was to test the benchmarking model on six real-life and ISO-certified risk management systems.

The **challenge** was to prepare, organize and conduct case studies that would provide solid scientific results about the efficacy of real operating risk management systems that are based on ISO management standards and have been shown to be successful, i.a., through third party certification audits or by a governmental regulator. More specifically, the challenge involved the following:

- a) Establish a first draft of the benchmarking model for a holistic approach to risk management systems based on ISO standards, both MSS and guidelines.
- b) Choose six real operating and ISO certified organizations in different industries to work with, make signed contracts with every one of them, get the organizations to nominate a contact person, and organize the case studies.
- c) Collect and review data (documents) regarding risk management systems in all six organizations.
- d) Conduct interviews in the form of audits according to the ISO 19011 auditing standard, to confirm data received from organizations and clarify issues.
- e) Apply the refined benchmarking model on all the data received in the six case studies.
- f) Writing the article and having contact persons and lawyers from the six organizations reviewing the text that concern their organizations and get approval for the publication of the article. Just the approval process took six months.

The **key contribution** of Article B consisted in the connection made between risk management systems in businesses and risk science. The benchmarking theory is used to develop a benchmarking model, based on risk issues discussed in recent scientific articles that

can be used to assess the efficacy of risk management systems in real ISO certified organizations. The efficacy of such risk management systems can be difficult to measure because ISO standards are not based on risk science and provide little guidance on how to do so. Due to the growing importance of risk management in all business operations, management, and use of standards, it is important to find ways to measure the efficacy of risk management in a better way than hitherto.

The **piece of insight** generated by Article B enabled a deeper understanding of a risk management framework, its limitations, and challenges. The article describes the development of the benchmarking model. It is divided into the following two steps:

Step 1: Validation and evaluation of the foundational elements of a generic risk management system that is based on ISO standards. Assessment template with a simple scoring system.

Step 2: Validation and evaluation of some of the most critical elements of the risk management process, according to ISO and scientific literature on risk management issues.

Step 1

An assessment template with a simple scoring system can be used to evaluate the existence of the basic elements of a risk management system. Based on the findings presented in the article the following benchmarks were defined. The scoring system provides a quantitative metric system with simple scores such as “yes”, “no”, “not applicable”, and “not specified”. The proposed benchmarks are as follows:

1. Scope, context, and boundaries of the risk management system.
2. Compliance with regulative requirements concerning the business.
3. Certifications.
4. Policies regarding risk are documented.
5. The risk management system is documented.
6. Risk analysis is conducted in a formal way.
7. Risk assessment is conducted in a formal way.
8. Risk (acceptance) criteria are set.
9. Residual risk is addressed (identified and assessed).

Step 2

If a risk management system meets the criteria in Step 1 and the benchmarks are positive, the next step is to assess the quality in terms of efficacy of individual elements of the risk management system. In this study, the most important elements of the risk management process were put in focus and findings in Section 2.3 used as basis for benchmarks.

To assess the scope further, context, compliance, and conformity of the risk management system (no. 1–5 in Step 1), the following benchmarks were defined:

1. Scope and outer boundaries of the risk management system.
2. Internal boundaries and interfaces, complexity of the organizational structure, and distribution of accountability.
3. Hierarchical structure with regard to risk, both safety and security risk.
4. Resources, knowledge, and experience needed to support the risk management system.

Additionally, the following benchmarks were defined to further assess the efficacy of

some of the most important elements of the risk management process (no. 6–9 in Step 1):

5. Risk analysis ability to capture complexity of the business operation and systems (foundation, method, technique).
6. Risk assessment ability to capture risk evaluation (ability to capture risk knowledge).
7. Risk criteria setting in risk assessment.
8. Identification and treatment of residual risk, risk that is left after formal risk mitigation/treatment.

Table 4 provides an overview of the benchmarks in Step 2. The first column shows the benchmark number, second column shows the benchmark name, third column shows the corresponding principle/framework/process in ISO 31000 [2].

Table 4. Benchmarks with correspondence to ISO 31000:2018.

No.	Benchmark Name	Corresponding Risk Management (RM) Principle/Framework/Process Clause in ISO 31000
1	Scope and outer boundaries of a RM system	Process (clause 6): Scope, context, and criteria (6.3)
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Process (clause 6): Scope, context, and criteria (6.3)
3	Hierarchical issues (layer issues, unclear hierarchical safety and security structure) within a RM system	Principles (clause 4): Structured, comprehensive, and dynamic RM Framework (clause 5): Leadership and commitment (clause 5.2) Process (clause 6): Risk assessment (clause 6.4) and risk treatment (clause 6.5)
4	Resources available to support the RM system	Framework (clause 5): Leadership and commitment (clause 5.2)
5	Risk analysis ability (foundation, method) to capture complexity	Process (clause 6): Risk assessment (clause 6.4)
6	Risk assessment ability to capture risk evaluation	Process (clause 6): Risk assessment (clause 6.4)
7	Risk criteria setting in risk assessment	Process (clause 6): Risk assessment (clause 6.4) and risk treatment (clause 6.5)
8	Treatment of residual risk, risk that is left after risk mitigation	Principles (clause 4): Continual improvements Framework (clause 5): Improvement (clause 5.7) Process (clause 6): Risk assessment (clause 6.4), risk treatment (clause 6.5), monitoring and review (clause 6.6)

The article provides insights into real risk management systems in organizations that have shown their commitment regarding professional management through accredited ISO certifications. All the organizations expressed their ambition to improve their risk management and be able to demonstrate the value of risk management, which can be difficult to evaluate. They are listed in Table 5. The piece of insight generated from Article B is best described in each case individually.

Table 5. Organizations examined in this study.

ID	Organization	Business Operation	Accredited ISO Certifications
A	Public health service	Processing of biological samples	ISO 9001
B	Public supply system	Operation of an electricity transmission system	ISO 9001, ISO 14001, ISO 45001
C	Construction company	Construction of an infrastructure facility	ISO 9001, ISO 14001, ISO/IEC 27001, ISO 45001
D	Manufacturing company	Manufacturing of a medical device	ISO 14001, ISO 13485
E	Software company	Software development	ISO/IEC 27001
F	Pension fund	Financial investments	ISO 9001, ISO/IEC 27001

Case A – A public health service: The public health service is an important part of the infrastructure of the country’s health system. It is not a competitive business entity, but the ISO certification shows ambition in operation and good service. The procedure for risk analysis is not yet fully documented. It is difficult to manage risk on the border of the business scope and risk related to communication. Lack of communication with external parties has been difficult to capture. It has also been difficult to communicate risk information to authorities. Table 6 presents a summary of the results from the public health service. The fourth column, “Hypothesis (True/False)”, refers to the hypothesis described in Article A, that certain risk issues will be evident in practice, provided a benchmarking tool (model) can be applied. If so, the hypothesis is true, otherwise it is false.

Table 6. Results from the public health service (case A).

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	Outer boundaries of RM system stretched into other health care institutions without compliance with ISO procedures	True
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Boundary issues regarding joint service and infrastructure of the hospital	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Two-dimensional risk metrics does not capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk criteria unclear	True
8	Treatment of residual risk	Residual risk not addressed	True

Case B – A public supply system: The public supply system is a critical infrastructure system. Risk analysis has revealed that electrical power security is insufficient in some places and breakdowns have led to power outages. The bottom-up risk analysis method has led to causal relationships between risk factors not being identified, the root cause has not been identified, and risk that does not clearly fall within one of the departments is not identified. Table 7 presents a summary of the results from the public supply system.

Table 7. Results from the public supply system (case B).

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	Risk associated with stakeholders not always addressed	True
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Internal boundaries well defined but bottom-up risk assessment within departments has led to causality between risk factors not being identified	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	Hierarchical issues found	True
4	Resources available to support the RM system	Resource issues found	True
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Two-dimensional risk metrics do not capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk criteria sometimes unclear	True
8	Treatment of residual risk	Not every known risk is included in the risk assessment and treated, therefore left as residual risk	True

Case C – A construction company: A single but complex construction project, executed by a governmental organization that lasted five years, was analyzed. Other parts of the organizations were not analyzed. Many contractors took part in the project. The company has been ISO certified to four management system standards for decades and its risk management system is mature. Through many comprehensive construction projects, the company has developed a strong risk management culture. The company's risk management leaders are therefore aware of the importance of risk analysis and risk management. Both the project risk manager and the company's risk manager believe that there are still opportunities to improve risk analysis and risk management within their company, e.g., with better coordination and integration into the company's overall management. Employees could be better educated and given better guidance in their work. ISO standards in general provide good support for risk management. The problematic question is: How much is a company willing to invest in the implementation and improvements of a risk management system? Key risk indicators need to be defined for indication of imminent risk. It is challenging to define what should be measured and monitored and it needs to be carefully done. Table 8 summarizes the results from the construction project. No issues were reported for benchmarks no. 5, 6, 7, and 8 in Table 8. This means that the hypothesis could not be verified.

Table 8. Results from the construction company (case C).

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	No issues reported	Not verified
6	Risk assessment ability to capture risk evaluation	No issues reported	Not verified
7	Risk criteria setting in risk assessment	No issues reported	Not verified
8	Treatment of residual risk	No issues reported	Not verified

Case D - Manufacturing company: The development and production of only one medical device was analyzed, not the whole business. It has taken the company many years to optimize their manufacturing processes for bionic medical devices. Safety must be built into the design and risk must be managed throughout both design and production phases. The whole process is based on continuous and iterative risk analysis. Risk analysis experts have gone to great lengths in their risk analysis to develop safe products and meet the requirements of regulators. The risk control system has been a burden at times, where regulators demand ever-increasing formality and documentation. Now, a balance in the cost effectiveness and the regulatory compliance has been reached. Applying ISO standards is one way of meeting requirements from regulators, supervising authorities, and buyers (that are typically not end-users). Despite limited guidance on risk management in ISO standards and inconsistency in their definition of important risk terms, the ISO standards are essential for the business. Table 9 presents a summary of the results from the development and production of a medical device. No issues were reported for benchmarks no. 5, 6, and 8 in the table. This means that the hypothesis could not be verified.

Table 9. Results from the manufacturing company (case D).

No.	Benchmark	Issues found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	No issues reported	Not verified
6	Risk assessment ability to capture risk evaluation	No issues reported	Not verified
7	Risk criteria setting in risk assessment	No issues found	False
8	Treatment of residual risk	No issues reported	Not verified

Case E – Software company: The software company conducts a detailed risk assessment and risk analysis in accordance with ISO/IEC 27001. The process and results from risk assessment are well documented and the questionnaire information is based on the certified ISO risk management system. The systems theory technique, STPA, is being used but has not yet been fully implemented in the risk analysis process. The use of risk management software ties the risk assessment, risk analysis, and the risk treatment to requirements and controls from ISO/IEC 27001. Risk calculations are performed in three ways to clarify and support risk management decisions. Various information is registered in free-text fields regarding asset properties, threats, likelihood, and vulnerabilities. This is to ensure that different parties within the company can assess the risk based on the same information and come to the same conclusion regarding risk. Despite the effort and the good awareness of the company's experts, it is their own assessment that various risk issues are present. Table 10 presents a summary of the results from the software company. It shows that only benchmarks no. 1 and 3 are without any issues.

Table 10. Results from the software company (case E).

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Internal boundaries sometimes unclear	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	Lack of resources	True
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Limited ability to capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk setting unclear	True
8	Treatment of residual risk	Residual risk partly addressed	True

Case F – Pension fund: The pension fund’s risk experts consider themselves well aware of financial and investment risk factors. This is confirmed by the fund’s good performance in previous years. However, some risk factors have not been identified, e.g., risk associated with hybrid threats and world threats, such as pandemics, environmental threats, democratic threats, technology transition (e.g., blockchain), and international politics. Future international investments require risk to be carefully assessed and aligned with the investment policy. Not only the expected return on investment must be considered, but also requirements from members regarding sustainability, environmental impact, and ethics. Therefore, risk analysis must not only be transparent, dynamic, and efficient, it must also be reliable and systematic in capturing new risk factors arising from present-day complex systems. Table 11 presents a summary of the results from the pension fund investments.

Table 11. Results from the pension fund (case F).

No.	Benchmark	Issues found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Risk assessment ability to capture risk evaluation is limited	True
7	Risk criteria setting in risk assessment	Risk criteria unclear	True
8	Treatment of residual risk	Treatment of residual risk unclear and residual risk not always addressed	True

The study described in Article B shows that ISO standards can be applied in many ways in risk management systems, depending on the nature of the operation and the business needs. Evidence, results, and testimonials in this study confirm that risk management is increasingly important for business, and it is becoming an integrated part of a management system. This is in line with findings in a former study, described in Article A. This study also shows that in all six cases examined, different approaches are taken to risk analysis and risk management. By applying the benchmarking model developed as described in Article B, it was possible to find both risk issues and risk factors that had not previously been found. The study provides evidence that despite the importance and good efforts, risk management and particularly the analysis of risk was not done satisfactorily in four out of six cases studied. Table 12 gives an overview of the risk issues found and in each organization. The first two columns show the number and the name of the benchmarks. The third column shows the correspondence of the benchmarks to the three parts of the ISO 31000 risk management guidelines, i.e., principles, framework, and process. Columns 4–9 show the findings in the organizations' risk management system. The last column shows the frequency of risk issues found based on benchmarking. The “x” means that issues were found in the risk management system, “ ” (a blank) means that no issues were found, “n.v.” means that risk issues could not be completely verified in this study. The last column shows the frequency of the risk issue (max 6). At the bottom of the table, the total number of risk issues found in every case is shown, max 8 risk issues in every organization A–F.

Table 12. Overview of the risk issues found and in which organizations.

No.	Benchmark	Corresponding to Risk Management (RM) in ISO 31000:2018	Risk Issues Found						Freq. of Risk Issues
			A	B	C	D	E	F	
1	Scope and outer boundaries of a RM system	Process: Scope, context, criteria	x	x					2
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Process: Scope, context, and criteria	x	x			x		3
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	Principles: Structured, comprehensive, and dynamic Framework: Leadership and commitment Process: Risk assessment and treatment		x					1
4	Resources available to support the RM system	Framework: Leadership and commitment		x			x		2
5	Risk analysis ability to capture complex systems and business operations	Process: Risk assessment	x	x	n.v.	n.v.	x	x	4
6	Risk assessment ability to capture risk evaluation	Process: Risk assessment	x	x	n.v.		x	x	4
7	Risk criteria setting in risk assessment	Process: Risk assessment and treatment	x	x	n.v.	n.v.	x	x	4
8	Treatment of residual risk	Principles: Continual improvements Framework: Improvement Process: Risk assessment, treatment, monitoring, and review	x	x	n.v.	n.v.	x	x	4
Total no. of risk issues found in RM system			6	8			6	4	24

“x” = risk issues found; “ ” = no risk issues found; “n.v.” = could not be verified in this study.

This can be summarized as follows:

1. Scope and outer boundary issues were found in 2 out of 6 cases.
2. Interface issues were found in 3 out of 6 cases.
3. Hierarchical issues were found in 1 out of 6 cases.
4. Resource issues were found in 2 out of 6 cases.
5. Issues regarding risk analysis ability to capture complex systems and business operations were found in 4 out of 6 cases.
6. Issues regarding risk assessment ability to capture risk evaluation were found in 4 out of 6 cases.
7. Issues regarding setting of risk criteria were found in 4 out of 6 cases.
8. Issues regarding residual risk were found in 4 out of 6 cases.

4.3 Article C

The **aim** of Article C was to investigate a relatively new methodology and techniques, still in development, for solving the objectives of a safety and security-based design of a major national infrastructure. The research objectives were tested on a specific project, a WtE project that can have significant and diverse impacts on people and the environment. It is

feared that it may have many safety and security issues unless they are considered from the beginning, as well as risks being identified and met appropriately during decision making at all stages of the project from the start. More specifically, the aim of this study was:

- a) To review the scientific literature on risk analysis conducted in recent WtE projects.
- b) To review recent literature on the application of STAMP, STPA, and STECA.
- c) To show how the STAMP accident causation model and the derived analysis techniques STPA and STECA can be applied to establish a system model that can then be used to confirm the concept, analyze the project risk, and define design requirements regarding risk in the early phases of the project.
- d) To compare the results from this study to the results from risk analyses presented in recent articles on WtE projects, see the literature review in Section 3.

The **challenge** was to identify and align actors and stakeholders and create a STAMP system model that shows all major system interactions regarding safety and security. To analyze them, all relevant laws, regulations, and rules, both national and European, had to be reviewed. It was also necessary to analyze all the communication regarding safety and security that is required at a given time in the process of decisions, preparation, and construction. Furthermore, the challenge consisted in finding representatives of these parties and having them confirm the system data.

The **key contribution** of Article C consisted in the combined application of STAMP, STPA, and STECA, a relatively new methodology and techniques for achieving the objectives of a safety and security-based design of a major national infrastructure. It was tested on the example of a WtE project. In this, many academic fields were involved, i.a., safety science, risk analysis, project management, stakeholder theory, systems theory, and social science. The focus, however, was on risk analysis and risk management. It is a challenge to design and build a major national infrastructure that is very costly, takes many years, and concerns all citizens of a country. The project not only needs to be financed, but it must also be supported by both the public and politicians. If executed, the project would also be an important step in making Iceland sustainable in waste management. In the article, Safe-by-Design (SbD) has been chosen as an engineering concept for risk management. It is a way to consider safety and security as much as possible from the beginning. Through communication, the SbD concept enables engaging different stakeholders throughout the development process and making their viewpoints and expectations understandable and transparent to each other.

The **piece of insight** generated from Article C was a system model of a WtE incineration plant with all relevant stakeholders and their interactions, feedback, and control actions, regarding safety and security. There were 26 stakeholders identified and they are listed in Table 13.

Table 13. List of stakeholders in the WtE project and their roles and responsibilities in the preparation and construction phase.

Stakeholder Id	Name of Stakeholders in the Construction Phase	Roles and Responsibilities of Stakeholders
S-1	Municipalities	<ul style="list-style-type: none"> • Legal obligation to dispose of waste in a sustainable way • Responsibility for establishing the proper governance in the preparation and early decision-making phase of the project • Project feasibility study • Project risk assessment • Responsibility for financing the whole project • Establishing the PPP for the project • Supervisor role
S-2	Waste Municipal Association (WMA)	<ul style="list-style-type: none"> • Serves the municipalities in establishing the WtE project • Knowledge source
S-3	WtE Ltd.—project owner	<ul style="list-style-type: none"> • Project owner (PPP affiliate) • Project mgmt., incl. quality, health and safety, environmental and sustainability requirements • Ensures project financing • Daily supervision during project time • Appoints a design manager • Appoints a construction manager • Assigns auditors • Applies for a construction permit for the intended project and provides the necessary data, e.g., environmental assessment
S-4	Ministry of the Environment, Energy and Climate	<ul style="list-style-type: none"> • Waste matters in accordance with the provisions of the regulatory framework for waste management, i.a., obligations under EEA law
S-5	The Environment Agency of Iceland	<ul style="list-style-type: none"> • Enforces laws on pollution prevention, environmental responsibility, nature conservation, and hygiene, sets environmental regulation • Issuance of operating license for the WtE plant
S-6	Municipality port	<ul style="list-style-type: none"> • Provides harbor facilities for shipping to and from the WtE plant location • Examines conditions for harbor construction
S-7	National Planning Agency	<ul style="list-style-type: none"> • Implementation of laws and regulations on environmental assessment of projects and plans • Presents the project owner's assessment plans and environmental assessment reports • Issues an opinion on assessment plans and on the environmental assessment of a project based on the developer's environmental assessment report and comments received on it
S-8	The Road and Coastal Administration	<ul style="list-style-type: none"> • Determines the roadway • Negotiates with landowners • Road design
S-9	Regulatory body for buildings and constructions	<ul style="list-style-type: none"> • Monitoring of the implementation and compliance with laws and regulations regarding building and construction • Investigation of whether building regulations are violated or not followed • Operation of a database for information on buildings and construction

S-10	Building licensor (municipality/landowner) of WtE construction site (many sub-institutions, fire brigade, health committee, planning committee, and politicians)	<ul style="list-style-type: none"> • Review of building permit application and building documents • Confirming consistency in the regional development plans • Granting a building permit • Investigation of major accidents and injuries • Work status checks
S-11	Parliament	<ul style="list-style-type: none"> • Makes legislation regarding waste disposal, environment, health and safety
S-12	European Union (EU)	<ul style="list-style-type: none"> • Coordinates waste and environmental issues within the EU • Working groups with the participation of individual countries
S-13	Investors	<ul style="list-style-type: none"> • Co-finance
S-14	Banks	<ul style="list-style-type: none"> • Co-finance
S-15	Main contractor	<ul style="list-style-type: none"> • Human resources available when needed • Necessary equipment available when needed • Project management on site • Tendering and selection of subcontractors • Project risk assessment • Coordination of subcontractors • Assesses, monitors, and manages risk on project site • Finishes the project on time
S-16	Subcontractors	<ul style="list-style-type: none"> • Subcontractors available on time • Risk assessment for work packages carried out • Professional knowledge and experience
S-17	Design manager	<ul style="list-style-type: none"> • Submission of design data/drawings for approval for a building permit application • Compiles a report on the designer's area of responsibility and confirms with their signature that it is a comprehensive overview • Handles the owner's internal control for the design of the construction • Organization of coordination of design data
S-18	Construction manager	<ul style="list-style-type: none"> • Makes written agreement with the master craftspeople which they hire on behalf of the owner • Carries out the owner's internal control from the time the building permit is issued until the final assessment has taken place • Carries out phased audits according to the inspection manuals • Professional representative of the project owner [S-3] • Requests a final audit before the WtE plant is started • Operation of a quality management system
S-19	Engineers, consultants, and designers	<ul style="list-style-type: none"> • Business plan • Risk analysis and risk assessment • Information gathering • Design of the WtE plant
S-20	Insurance companies	<ul style="list-style-type: none"> • Insurance
S-21	Auditors, inspection agencies, e.g., the Government Property Agency	<ul style="list-style-type: none"> • Auditing standards and process • Financial auditing • Health and safety, quality, security, and environmental management auditing • ESG auditing

S-22	The public	<ul style="list-style-type: none"> • Approve of the project • Remain critically engaged
S-23	Parties of the labor market	<ul style="list-style-type: none"> • Preserve peace in the labor market
S-24	Electrical grid company	<ul style="list-style-type: none"> • Provides a connection to an electricity transmission system through a substation • Transmits electrical power generated by the WtE plant to buyers
S-25	Hot water distribution company	<ul style="list-style-type: none"> • Provides a connection to the hot water distribution system • Distributes the hot water coming from the WtE plant
S-26	Concrete plants and tarmac production units (buildings and roads)	<ul style="list-style-type: none"> • Use of good and affordable building materials

The STAMP system model with its control structure of the WtE project is shown in Figure 8. A STAMP system model with its control structure for the WtE project. The actual project, the construction of the WtE incineration plant, is the controlled process and is shown with the red color in the bottom half of the figure. The model is not presented in a hierarchical form but is organized with regard to time factors in the project, with early involvement shown from the top and later involvement towards the bottom. The figure shows 26 stakeholders (listed in Table 13) displayed as gray-colored controllers and one red-colored controlled process. Figure 8 shows a simplified interaction that consists of necessary feedback and control actions occurring between stakeholders.

Figure 8 shows that the project owner plays a central role in the system and the project. Until the project owner group has been established, the Waste Municipality Association (WMA), stakeholder S-2, functions as a think tank and drives the project forward – it is already responsible for processing more than half of all waste in Iceland. Six municipalities in the capital area of Iceland, representing 63% of Iceland’s population, build the owner group of the WMA. They are marked as stakeholder S-1 in the STAMP model. They play a leading role in the preparation phase of the project, together with S-2. The business is controlled by politically elected representatives, with authority for only four years at a time. These two stakeholders do not have the financial resources to execute this project alone. Therefore, a partnership of public and private investors is needed. A review of current laws on waste management and the responsibilities and duties of municipalities reveals uncertainties in many aspects of this kind of project.

The STAMP system model shows the feedback every stakeholder needs to give, with broken arrow lines, to fulfill their roles and responsibilities. In the same way, the control action required from each stakeholder is shown with an unbroken arrow line. For the project to be interesting to investors, the flow of material for incineration must be guaranteed. In most countries, the products of the incineration plant will be in demand for energy buyers, both electricity and hot water. In Iceland, however, there is already enough supply of both electricity and hot water at a relatively low price. The motivation is, therefore, primarily for the country to be sustainable regarding waste management and independent from other countries. This makes it a more challenging business plan. Stakeholders S-13 and S-14 are needed to finance the project, but they need assurance for their investment. The municipalities also need assurance that the project will be completed, and that the incineration plant will be able to fulfill their duties regarding waste management. The next step in the modeling process is, therefore, to focus on how this challenge can be met and to take a closer look at the project owner function, i.e., stakeholder S-3.

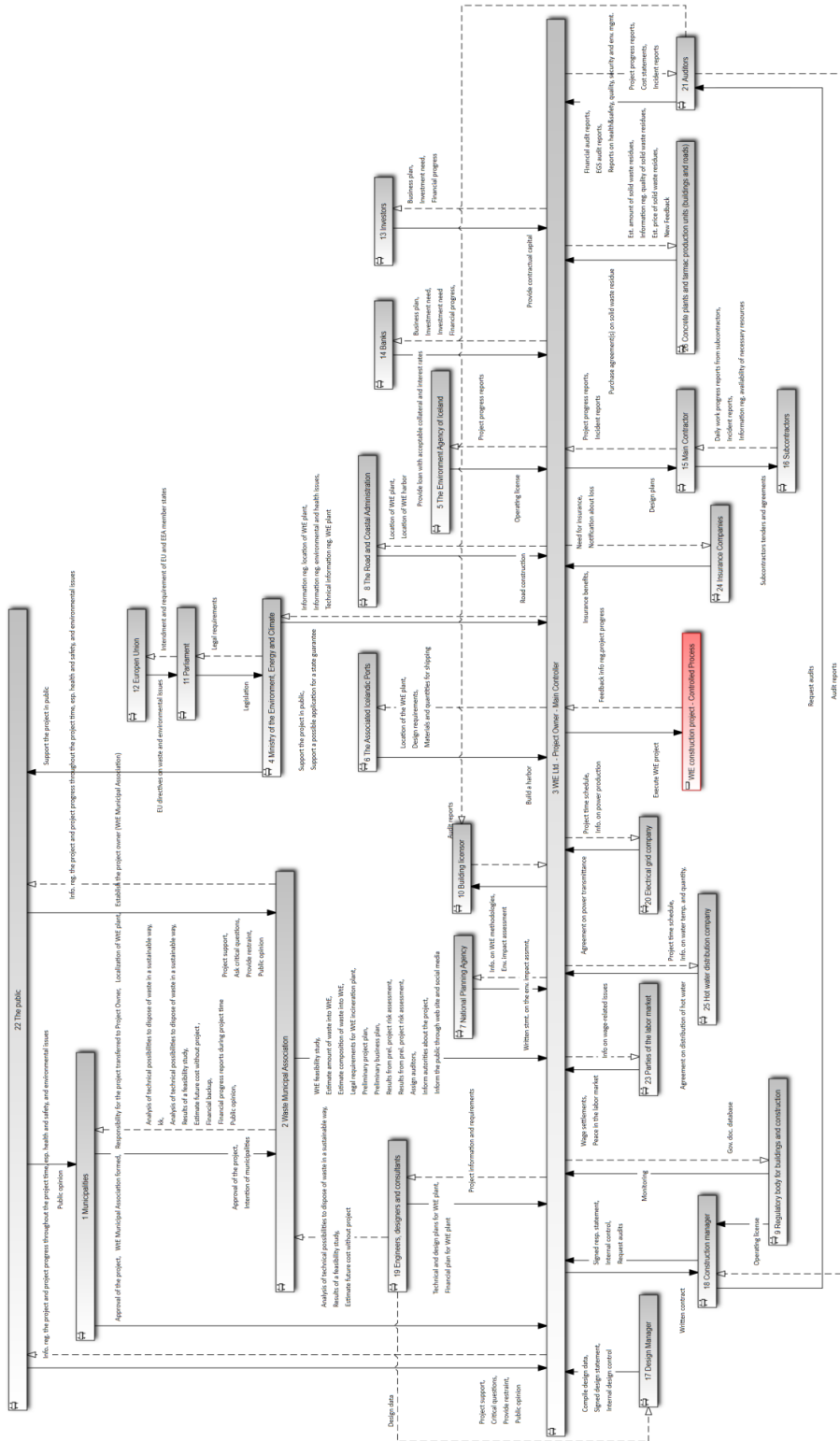


Figure 8. A STAMP system model with its control structure for the WtE project.

Iceland's waste management is governed by Act No. 55/2003, which places an obligation on local authorities to operate reception and collection centers, sometimes referred to as disposal sites. This legislation also sets limits on the WMA (stakeholder S-2) disposal of household waste. Public procurement projects of governmental entities are subject to tender as per Act No. 84/2007, contingent on circumstances within the European Economic Area (EEA). Additionally, the activities of the WMA are governed by Act No. 44/2005 on competition, which prohibits the abuse of market-dominant and monopoly positions.

It is plausible to consider that the already existing WMA could serve as the proprietor of an incineration plant. This aligns with the legal mandate for municipalities to establish waste management channels. The rationale supporting an incineration plant mirrors that of the existing landfill's operation. This holds true even if the incineration plant operates under a distinct WMA organization as an autonomous business unit, maintaining compliance with the same legal framework.

The existing WMA is equipped to oversee the incineration of all household waste, given municipalities' obligation to collect and manage it. On the other hand, waste from businesses and industries is handled by private entities. Consequently, maintaining competitive gate fees becomes a crucial requirement. As the activity falls under the purview of Act no. 44/2005 on competition, careful steps must be taken when implementing measures to secure a steady supply of waste for the incineration plant. Incineration of waste for the WMA (S-2) is subject to tender in the EEA (S-11 and S-12) unless the association takes care of it itself. An exemption from this is granted if the operator of the incineration plant is a public entity and if 80% of the plant's projects are assigned to the plant by public entities.

The first steps taken here with the STAMP modeling of the WtE project, and preliminary risk analysis with STPA and STECA, highlight the assumptions that must be laid as a basis for a project like this. Based on the assumptions of the project stated here, the following five scenarios can be thought of as possible advantages for the WtE project owner in terms of structure or setup of the project:

1. Public ownership, implementation, and operation.
2. Public ownership, but private implementation/execution and operation.
3. Private ownership and implementation/execution, but public operation (property leased to a public entity).
4. Mixed ownership of implementation/execution and operation.
5. Private ownership, execution, and operation.

After the first review of these five scenarios by stakeholder S-2, it seems that the third scenario is the most favorable. This result was obtained with the help of the STAMP model and, with its control structure, delineated the first STPA step (see results in Table 13) and iterated safety/security communication and interaction protocols between stakeholders and actors using the STECA technique. This process made it easier for people who participated in the analysis to sharpen their focus and capture the essential parts of the system at this point; see a list of interviewees in Article C, Table A1 in Appendix A. Examples of questions and answers from interviewees are presented in Article C, Table A2 in Appendix B. During meetings with stakeholders and actors where the system-level constraints were scrutinized, the five scenarios were defined and analyzed. The scenario analysis included a closer look at the possibilities for minimizing the system risk and obtaining the most favorable ownership arrangement. This examination resulted in choosing scenario 3 as the best solution.

Scenario 3 involves private ownership and suggests that the project is financed with

equity capital and a construction loan. The scenario also implies that the operation will be public and that access to household waste is guaranteed. The risk factors in this scenario, at this stage, are related to (1) social risk and (2) risks related to investors and contracts with them; projects like this offer green investment potential, but investors are likely to want to minimize their risk with a turnkey contract project arrangement. (A turnkey project is constructed such that it can be sold to any buyer as a completed product. The Cambridge Dictionary provides a definition of a turnkey contract: "A contract in which a company is given full responsibility to plan and build something that the client must be able to use as soon as it is finished without needing to do any further work on it themselves" [122].)

Extensions of Table 13 is given in Article C, Table A3 in Appendix C.

4.4 Article D

Article D is a conference article that was published at the 5th European STAMP/STPA workshop and conference at Reykjavik University in 2017 to present results from a STPA software development project that was done in collaboration with Stiki and ZHAW and funded by Eurostars. It became a part of this thesis work to manage this three-year project. The **aim** was to investigate the modeling process of multiple levels of abstraction in hierarchical control structures and the application of STPA. The aim was furthermore to clarify the design of a STPA software tool that could be used in the case studies conducted in this thesis and thus clarify the functionality of the STPA process and thereby be supportive in all steps of the analysis work.

The **challenge** was diverse. In STPA a control structure is created as a functional system representation and used as a model and a starting point for the hazard/threat analysis itself. The development of the control structure usually involves multiple iterations. This modeling work typically starts at a rather abstract level but is then refined during the modeling or at later stages in the analysis process. It was a challenge to differentiate between model and views and investigate ways to allow the use of multiple diagrams when representing one model. Usually, no differentiation is made between the control structure model and its representation as a diagram. Normally, the representation is restricted to a single control structure diagram. In addition to this it was also a challenge to manage the Eurostars project and to find the right graphical tool to realize the modeling process and connect information entities from the model to the STPA analysis itself and the creation of scenarios used to analyze unsafe control actions.

The **key contribution** of Article D consisted in developing a usable STPA tool to support the STPA work. The article introduces the concept of using multiple diagrams to represent one model of the control structure. This is especially useful for software editors dedicated to STPA analysis. It also addresses the opportunity of explicit differentiation between models and views in the form of diagrams.

The **piece of insight** generated from Article D was the importance of having clear rulesets when using multiple diagrams to represent one model. It provides insight regarding consistency issues, e.g., that the control structure representations are consistent with the model and with each other, and how to ensure the completeness of the analysis. While the rulesets for the individual use cases have been derived and a successful preliminary verification of them was conducted, the consolidation of the rules needs further investigation. In 2023, work began on the redevelopment of the STPA software solution as a SaaS web solution. This work is well underway. It is however a future work to continue this work and find ways to finance it. If it is possible to keep the project going, the intention is to continue the research regarding the consolidation of the rules described in Article D.

The concept described in this article is especially useful when diving into the details of a system. Making sure to comply with the ruleset and constraints involves some effort. However, this effort is highly automatable through software tools and does therefore not necessarily result in substantial additional workload for the analyst. Nevertheless, the analyst must understand the basic concept of modeling control structures, especially hierarchical control structures, with multiple diagrams. A ruleset with constraints allowing complementing views has successfully been implemented in the STPA software tool⁴.

The basic four steps of STPA, as described in Figure 3 can be summarized as follows:

⁴ <https://www.riskmanagementstudio.com/stpa-software-solution/>

1. The scope and the purpose of the system which is to be analyzed must be defined. Part of this step is to define system level hazards and losses which the analysis aims to prevent. The STPA can be applied to ensure safety, e.g., prevent loss of human life, or it can be applied to preserve security, privacy, performance, and other properties.
2. A model describing the system needs to be developed. This system model is typically described as a control structure – often a hierarchical control structure. The aim of the control structure is to break the system down into system elements, to identify controlling elements (controllers) and controlled processes, and to capture interactions and functional relationships between all the model elements as a set of control loops. The control structure represents a model of the system under analysis, system elements affecting safety, security, privacy or other properties, and the flow of control actions and feedback among those elements. Development of the control structure is the same for all properties and can be seen as preparation work before performing the actual analysis. The modeling usually begins at a very high and abstract level. The model is then iteratively refined to capture more system details as needed.
3. After developing the control structure, the model is used to systematically identify and describe inadequate and unsafe control actions, i.e., control actions that could lead to the previously defined system level hazards/threats and through this to the losses. If a control action can potentially lead to a system level hazard, it is categorized as an unsafe (or unwanted) control action. Every unsafe control action is used to define functional requirements and constraints for the system. This step is the same regardless of the properties STPA is being applied to.
4. Every control loop of the control structure is finally systematically analyzed to identify loss scenarios. The aim here is to find out why and how inadequate control actions, resulting in unwanted process outcomes, can occur. Scenarios that can lead to losses are identified and used to improve system design, define additional requirements, and define mitigating control actions and feedback as described in the STPA Handbook [13].

The first draft of the control structure of a system to be modeled and analyzed should be at a rather abstract level. The control structure is usually in a form of a single diagram, even a single control loop, and without any system details as demonstrated in Figure 9. In the case of cancer treatment such an abstract representation may for example feature “Health service” as a single controller and “Patient health” as the controlled process, to begin with. At this initial stage, none of the internals of the “Health service” have yet been modeled individually. Examples of different levels of abstractions can be found in the literature [123],[124].

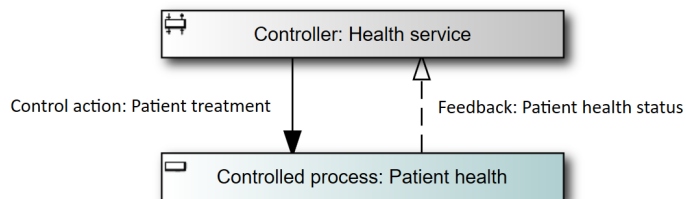


Figure 9. Generic control loop of a health service.

There are several reasons for starting modeling at a high and abstract level. The following four points illustrate the modeling process:

1. The same applies to STPA as other risk analysis methods, the scope of the analysis needs to be determined at the beginning. The development of the control structure covers one aspect of this “scope definition”. Starting the modeling process at an abstract level makes it possible to define the scope roughly right from the start. Through progress of the analysis and refinement of the abstract control structure representation, the scope will also gradually become refined.
2. When a system is used in different applications, an analysis based on an abstract representation may serve as a common starting point for individual, application specific analyses, and refinements. Consider a robotic arm used to weld metal plates, but also used for exchanging tools of a milling machine. STPA can be performed for the robotic arm itself, not considering the specific application. This analysis can be used as a starting point for further application specific analyses such as for the welding or tool exchange.
3. An abstract representation of a system may be valid for different types of systems. The same abstract representation may for example be used to model cancer treatment with proton radiation beams [125], [126], [127], [128] and brachytherapy [124], [129]. This means that existing models may be re-used and again serve as a starting point for more concrete analyses.
4. Finally, starting the modeling process at an abstract level allows the analyst to quickly identify those parts of a system for which further clarification activities are necessary. This is relevant since such activities typically require time. The sooner the clarifications are initiated the better.

While progressing with the analysis the original abstract representation is typically “discarded”, i.e., it is no longer actively considered for STPA, but instead more detailed, refined representations are used. Although the initial abstract representation might be kept for traceability reasons, as informative resource (in the simplest form the analyst may keep a printout of the control structure diagram), STPA currently foresees no formal way of maintaining multiple levels of abstraction. Such formal approaches would be especially useful for the creation of an STPA editing software tools and to ensure traceability. The key features that enable modeling a control structure by means of multiple diagrams are simple to state:

- Allow representation of a control structure by means of multiple diagrams (views).
- Allow using the same element in multiple diagrams.
- Allow parent-child relationship among elements.

However, as mentioned above, keeping the diagrams consistent and making sure STPA steps 3 and 4 match the model and are complete, is not trivial. The three diagrams presented in Figure 10 give an illustrative example of this complexity. The figure shows a representation of a control structure by means of three diagrams: Diagram 1, Diagram 2, and Diagram 3. To keep the diagrams consistent and ensure that the analysis matches the model and that it is complete, a ruleset and consistency considerations are indispensable.

1. Diagram 1 shows a control structure with three controllers labelled A, B, and C. It also shows a “Controlled process”. In this example only two control actions are explicitly shown, “Control action 1” and “Control action 2”.

2. Diagram 2 shows controllers A and B, and the same “Controlled Process” again. This diagram neither shows “Controller C” nor “Control action 1” which is received by “Controller C”.
3. Diagram 3 shows another view of the same model, now focusing on the internals of “Controller B”. Note that “Control action 1” appears on the first diagram, but it does not appear on the second and third diagram. Furthermore, the source of “Control action 2” is “Controller B” in the first and second diagram while it is “Controller B2” in the third diagram.

This brings up a couple of questions regarding the modeling and analysis process. For example:

- How is the analyst made aware of the fact that “Controller B” issues “Control action 1” when working with Diagram 2?
- Could the analyst show “Control action 1” on Diagram 2 even though “Controller C” is not represented?
- Is it inconsistent to have “Control action 2” appearing on Diagram 2 and 3 with different sources?
- How does “Control action 2” need to be handled in forthcoming steps of STPA, i.e., steps 3 and 4?

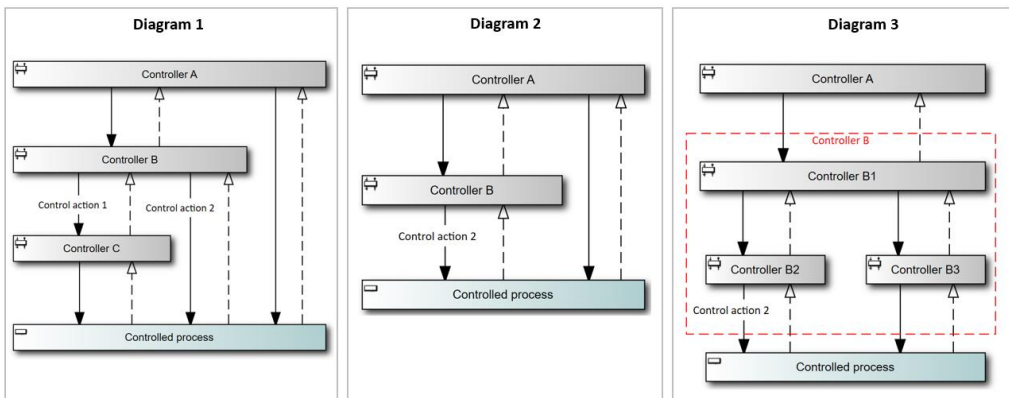


Figure 10. Representation of a control structure by means of three diagrams.

To ensure that all the diagrams are consistent, and the analysis is complete, a set of rules and consistency criteria are necessary. This does not only apply for the modeling work in step 2 of the STPA analysis process but also for the other steps in the analysis process. The approach illustrated in Figure 11 can be used to derive rulesets and consistency criteria for the individual use cases and consolidate them into one complete ruleset.

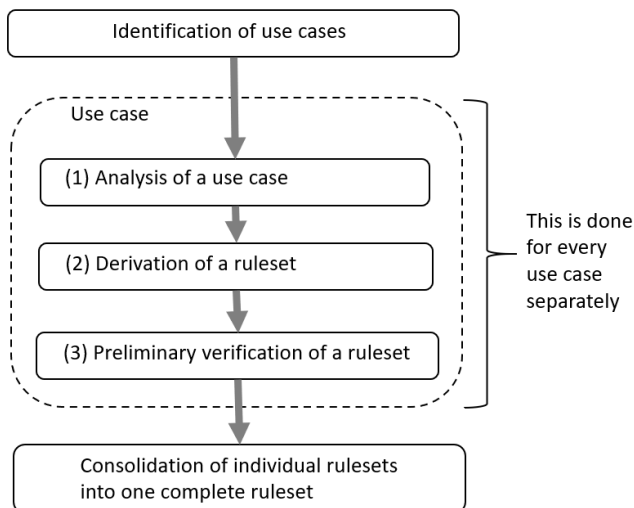


Figure 11. The process of establishing one complete ruleset.

To begin with, use cases of multiple control structure diagrams describing the same model were identified, as described in Article D. As a next step, the use cases were mentally played through and analyzed with the help of analyses from previous projects, literature and a constructed example [128], [130], [131]. The aim of the constructed example was to analyze situations which did neither occur in previous projects, nor were analyzed in the literature, but are principally possible. For each use case the set of rules was derived that is necessary to enable the use case. The set contains rules about modeling and consistency considerations but also rules influencing STPA steps 3 and 4. Previous projects, literature, and other examples were used to preliminarily verify the applicability and correctness of the derived ruleset. The individual rulesets were consolidated into one basic ruleset and the rules and consistency considerations refined, as necessary.

Introduction to complementing views

Figure 12 provides an abstract example of complementing views. Diagram 4 represents the exact same model as Diagram 4a and Diagram 4b together. However, two diagrams are used instead of one. “Controller R” generates “Control action 1” that is received by “Controller S”. “Controller S” generates “Control action 2” that is received by “Controlled process T”. Additionally, “Controller S” influences the “Controlled process T” directly by means of “Control action 3” and “Control action 4”. Feedback is not explicitly modeled in this example.

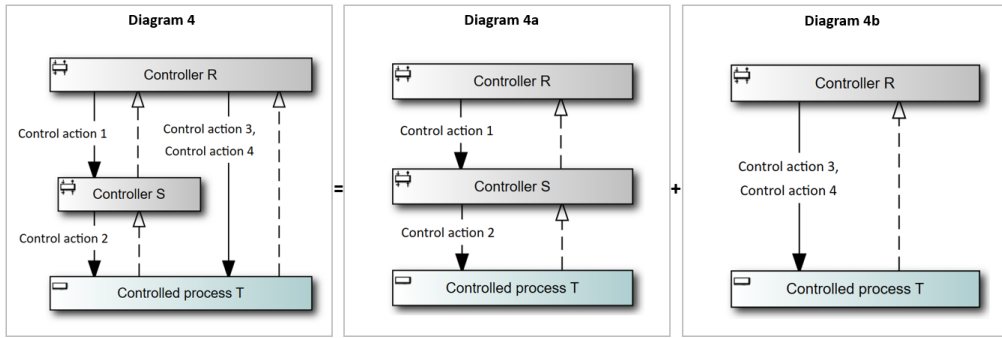


Figure 12. An abstract example of complementing views.

Figure 12 depicts a relatively simple control structure. Control structures are often more complicated, and it is advantageous to set up a table that highlights the appearance of elements in complementing views. Table 14 is an example of such a table for the views in Figure 12.

Table 14. Appearance of elements in diagram 4, 4a, and 4b in Figure 12.

Element	Appearance in Figure 5		
	Diagram 4	Diagram 4a	Diagram 4b
Controllers:			
Controller R	Yes	Yes	Yes
Controller S	Yes	Yes	No
Controlled Process:			
Controlled process T	Yes	Yes	Yes
Controlled Actions:			
Controlled action 1	Yes	Yes	No
Controlled action 2	Yes	Yes	No
Controlled action 3	Yes	No	Yes
Controlled action 4	Yes	No	Yes
Feedback: (Not treated in this example)			

Rulesets for complementing views

The rules identified for this use case are rather trivial and straight forward. A subset of those rules is provided in the following list:

1. The same controller may appear on multiple diagrams.
2. A diagram may represent only a subset of the control actions generated or received by a controller.
3. Identification of unsafe control actions (Step 3 in the STPA process, see Figure 3) needs to be performed for all control actions regardless of which diagram they are represented in.
4. Every element (controller, controlled process, control action, or feedback) must appear on at least one diagram.

This is a rather basic and straight forward use case. This ruleset for complementing views can not only be beneficial to the analyst in certain circumstances, but it is also a pre-requisite for all other use cases such as levels of abstraction addressed in the following section.

Introduction to levels of abstraction

This use case is based on the premises that two visual representations of a controller exist. The representations are based on [125] and shown in Figure 13. The figure shows two diagrams, Diagram A and Diagram B. Both diagrams are an example of the same health treatment, but they show two levels of abstraction of the controller “Treatment delivery” and the control action “Define treatment”. The control structure shown in Diagram B shows the internals of “Treatment delivery” in Diagram A. In Diagram B is the control action “Define treatment” furthermore refined into the control actions “Specify irradiation” and “Specify therapeutic requirements”.

To summarize, the two representations shown in Figure 13 are:

- A. A representation in Diagram A that shows the controller’s interaction with its environment. This representation shows the controller “Treatment delivery” without showing any internals of the controller itself.
- B. A representation in Diagram B that shows the internals of the controller “Treatment delivery”. In this representation the decomposed controller is visualized as a frame with red broken lines. Within the frame is the refined control structure with new elements and their control flow. It corresponds to the single controller “Treatment delivery” in Diagram A.

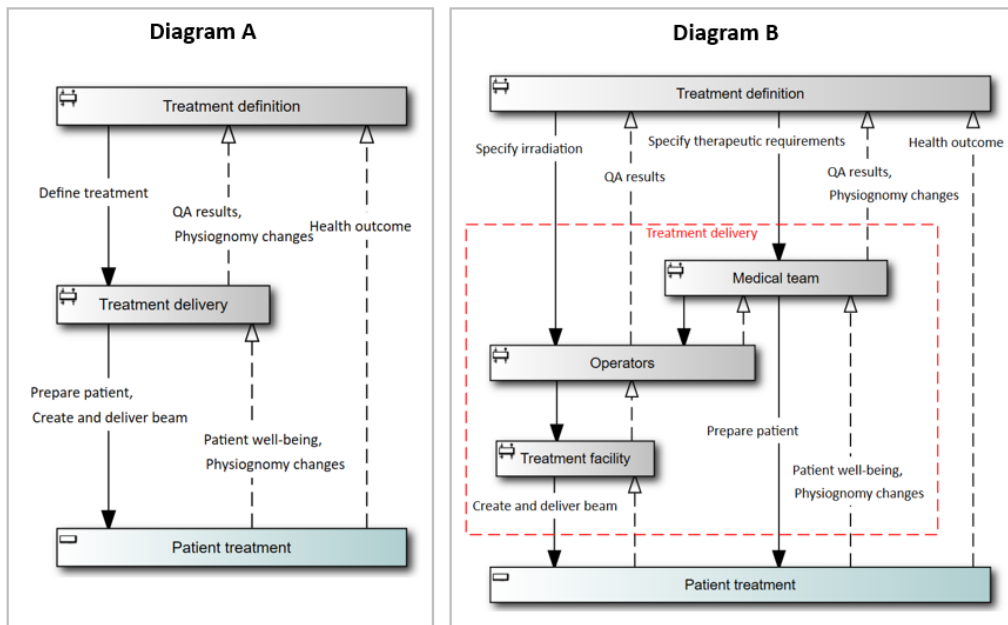


Figure 13. Two examples of the same controller showing two different levels of abstraction [125].

While Diagram A in Figure 13 displays the controller “Treatment delivery” as a single

unit, Diagram B displays the internal make-up of the “Treatment delivery”. These internals are the controllers “Medical team”, “Operators”, and “Treatment facility”. While the control actions “Prepare patient”, and “Create and deliver beam” are issued by the controller “Treatment delivery” in Diagram A, they are issued by the controller “Treatment facility”, respectively by the “Medical team” in Diagram B.

The concept of refinement does not only apply to controllers, but also to control actions and feedback. For example, Diagram B shows the control action “Define treatment”. This control action is not shown in Diagram A, but it is represented by the control actions “Specify irradiation” and “Specify therapeutic requirements”. An overview of the refinement and the relationship between controllers, control actions, and feedback is given in Table 15.

Table 15. Appearance of the Control Structure Elements in Figure 13.

Element		Appearance in Figure 6	
Parent Element	Child Element	Diagram A	Diagram B
Controllers:			
Treatment definition		Yes	Yes
Treatment delivery		Yes	As frame
	Medical team	No	Yes
	Operators	No	Yes
	Treatment facility	No	Yes
Controlled process:			
Patient treatment		Yes	Yes
Controlled actions:			
Define treatment		Yes	No
	Specify irradiation	No	Yes
	Specify therapeutic requirements	No	Yes
Prepare patient		Yes	Yes
Create and deliver beam		Yes	Yes
Feedback:			
QA results		Yes	Yes*
Physiognomy changes		Yes	Yes**
Patient well-being		Yes	Yes
Health outcome		Yes	Yes

* Feedback appears twice in Diagram B, once linked to "Operators" and once to "Medical team".

** Feedback appears twice in Diagram B, once linked to "Patient treatment" and once linked to "Medical team".

Rulesets for levels of abstractions

A pair of rules has been identified for the use case “Levels of abstraction”. They are as follows:

1. Feedback may have multiple sinks, i.e., the feedback may be received by more than one controller.
2. If feedback has multiple sinks, it must be related to each other by a parent-child relationship.

These two rules apply to the feedback “Patient well-being” in Figure 13. The sink of this feedback is the controller “Treatment delivery” (in Diagram A) respectively, but more precisely, the controller “Medical team” (Diagram B) is related by a parent-child relationship with “Treatment delivery”.

In the software development of the STPA software tool (the Eurostars funded project) that took place in parallel with this analysis process, a graphical software function was designed that defines all system components as unique entities and saves them in a database with unique identifiers. In this way, it is possible to reuse all system components in different diagrams and then inherit the properties of system components between diagrams. Individual feedback and control actions are also stored in the database with unique identifiers and can be reused in different diagrams. The user of the software is still responsible for putting together a diagram with the correct system components and interaction (feedback or control action). It would be interesting to explore the opportunity through further software development, to design automated consistency tests to verify consistency of a STAMP system model built from many specific model components.

4.5 Article E

The **aim** of Article E was to investigate whether the VUCA meter can improve the conventional risk identification process. The aim was furthermore to investigate if the VUCA meter can supplement the conventional risk identification process by capturing Black Swan events in the domain of projects and project management. As the world is confronted with the enormous responsibilities related to, e.g., geopolitics, climate change, energy adaptation, and social media, the isolation of risk that can harm sustainability seems imperative. The research was done by selecting one large project currently under planning and testing the VUCA meter.

The **challenge** was to get experts involved in the chosen project to take time and to participate in two workshops held at Reykjavik University. Several focus questions were designed for each workshop. The purpose of the first workshop was to perform a risk identification and risk assessment based on the traditional framework presented in the PMI Standard for Risk Management in Portfolios, Programs, and Projects [18]. The purpose of the second workshop was to apply a new method for identifying and assessing risk based on the VUCA meter presented by Fríðgeirsson and Ingason et al. [16].

The **key contribution** of Paper E consisted in contribution to the development of the VUCA meter. The conventional probabilistic and event-based approaches to risk assessment are great and have proven their usefulness. They do, however, have their limitations, especially when it comes to unprecedented events involving low-probability/high-impact risks, system risks, and risks that are less technical and more psychological/social in nature. Noteworthy is the study by Ackermann et al., who presented the “risk filter” that uses insights from forensics to identify risk exposure on future projects and tackle them [132]. Another study stating the difficulties of the conventional approach is by Qin et al. [133]. Titko et al. did an interesting study on how the escalation and severity of natural disasters will affect the public and the need for new ways to approach the incurred risks [134]. Lastly, the cognitive theories of Kahneman and Tversky on human limitations of decision making should be mentioned, see, e.g., [135], [136], [137]. The conventional method is an open approach relying on the experience and the cognitive state of mind of the participants. The VUCA meter is a normative approach that asks questions in a certain context. For the conventional workshops, five questions related to the conventional topics of a risk

identification process were used to elicit risk factors, one at a time. In the VUCA workshops, 20 focus questions were used to elicit risk factors, five questions for each component part of VUCA. In this case, five focus questions were answered at a time. The results indicate that the VUCA method might be a better way to force people to think somewhat beyond the traditional framework used for identifying risk factors in a project. The traditional framework included operational, financial, legal, regulatory, and strategic risk, but projects in modern times are faced with risk that is not necessarily encapsulated by this framework. Furthermore, the VUCA method may help to bypass cognitive biases that are well known sources for risk, see, e.g., the landmark studies of Kahneman and Tversky [135]. The risk factors that were captured using the VUCA method but not with the conventional method were of different kinds. Still, most of them seem to be related to the social and the environmental part of the project. This is the outcome of a framework that directed the participants to think of risk factors that occur as a result of the time of volatility, uncertainty, complexity, and ambiguity.

The **piece of insight** generated from Paper E was the comparison between the conventional PMI risk identification process on one hand and risk identification with the VUCA meter on the other hand. These two risk identification methods provide different results. The number of risk factors obtained by using the conventional method was 51 compared to 119 risk factors when using the VUCA method. This is a huge difference given that the time for both workshops was identical. The only difference between the workshops was the work process; the approach that was used to elicit answers from the participants.

The importance of risk management in the context of project management has been widely discussed in the existing scientific literature [138], [139]. All the tools and techniques used in risk management for projects are designed to help ensure that the project's delivered results are as expected and within identified constraints for the project. In the generic life cycle of projects, it is considered most effective when the risk events are identified and dealt with at an early stage of the project to be able to avoid big problems occurring in the project and to be aware of the risk events throughout its life cycle [140]. The risk management process is mainly divided into six steps: (1) Risk identification, where all possible risks that can have a negative impact on the project are identified; (2) risk assessment, including risk analysis, to determine which factors are the most important (riskiest) ones for the project; (3) a strategy and corresponding actions are developed and implemented to mitigate the risk; (4) monitoring and control of the risk; (5) report and integration against the risk; and (6) support for risk management, for example, with periodic project and risk meetings [141].

In this article, the emphasis is mainly on the first two steps of the risk management process, where the risk events are identified and assessed. This is carried out using tools and techniques such as expert judgment, data gathering, data analysis, interpersonal and team skills, prompt lists, and meetings. Many of those involved in a project can contribute to the risk identification process, e.g., the project team members, customers, project manager, operations managers, stakeholders, end-users, and of course, the project risk specialist if assigned. Generally, the risk assessment is done by assessing on one hand the likelihood of a risk event occurring and on the other hand the impact of the same risk event on the project [18]. This conventional open approach to assess risk as described above has been disputed and there are several scientific studies where it has been argued that this approach does not capture all the risk events that may affect the project, and significant risk events may be overlooked by using the conventional risk assessment techniques only [16], [132], [142], [143]. This is because the likelihood of events to occur is one of the critical variables in the calculation when assessing the most significant risk events for the project. A case study from

2007 [132] discussed this systemic risk assessment. The authors argued that the most attention in the systemic risk assessment is devoted to the technical risk in projects, not other risk categories such as political risk, customer risk, partner and supplier risk, human risk, reputation risk, market, and financial risk. A passable description of the characteristics of a risk event that might surpass the conventional risk assessment procedure based on the work of Nassim Taleb [5] is provided by [144] and shown in Table 16.

Table 16. The criteria for a Black Swan event adapted from [144].

Emergency response to the problem and fixing the problem are different aspects.
A solution to the problem is unknown and must be created under dismal circumstances.
Public relations issues can be massive, putting pressure on reputation, credibility, and perception of the public.
Governmental and regulatory agencies may demand response.
Productivity and cash flow may be affected negatively, liquidity could become uncertain, and asset prices disturbed.
Despite the problem, the day-to-day operation must continue.

4.6 Other publications and results from this thesis work

In addition to publications of Article A, B, C, D and E, the results of this thesis work have been published in conference proceedings, several master's projects have been completed as part of this thesis, and posters have been prepared and published at conferences. The most important product of the thesis work, however, is the STPA software developed in collaboration with ZHAW. A 3-year Eurostars grant was received for that project. The software development was important because of the fundamental work done in the software design process, but many issues had to be clarified and ruleset defined for the STPA software, from model building to scenario analysis.

The conference presentations are listed in subsection 4.6.1, the Master Theses are listed in subsection 4.6.2, and a short summary on the STPA software development is given in subsection 4.6.3.

4.6.1 Conference presentations

Here is a list of conference presentations that are part of the thesis work:

1. Title: **Comparison of Risk Analysis Methodologies – Risk Analysis for Better Design and Decision Making** [145].
Author: Svana Helen Björnsdóttir.
Presented at the 5th MIT STAMP Workshop, 23-26 March 2015, Cambridge, USA.
2. Title: **Comparison of Risk Analysis Methodologies in an Electrical Grid** [146].
Author: Svana Helen Björnsdóttir.
Presented at the 3rd European STAMP/STPA Workshop and Conference at Amsterdam University of Applied Sciences, 4-6 October 2015, Amsterdam, The Netherlands.
3. Title: **Risk Analysis in Design and Construction of a Hydropower Station** [147].

Author: Svana Helen Björnsdóttir.

Presented at the 4th European STAMP/STPA Workshop and Conference at ZHAW, 13-15 September 2016, Zürich, Switzerland.

4. Title: **STPA Software Module: A Eurostars funded software project** [148].
Authors: Christopher Brown, Jianfei Zheng, Svana Helen Björnsdóttir, Martin Rejzek.
Presented at the 5th European STAMP/STPA Workshop and Conference at Reykjavik University, 13-15 September 2017, Reykjavík, Iceland.
5. Title: **The Challenges of Supporting STPA with a Software Tool** [149].
Authors: Martin Rejzek, Svana Helen Björnsdóttir and Christopher Brown.
Presented at the 2018 MIT STAMP Workshop at MIT, 26-29 March 2018, Cambridge, USA.
6. Title: **STPA in Pension Fund Investments**.
Author: Svana Helen Björnsdóttir, Páll Jensson and Saemundur E. Thorsteinsson.
Presented at the 7th European STAMP/STPA Workshop and Conference at Aalto University, 17-20 September 2019, Helsinki, Finland.
7. Title: **Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk**.
Author: Svana Helen Björnsdóttir
Presented at the 14th Safety Gala virtual workshop in Athens, 5-6 April 2022, Athens, Greece.
8. Title: **The various facets of risk – Proposed WtE project in Iceland** [150].
Author: Svana Helen Björnsdóttir
Presented at the IMaR 2022 (Innovation, Megaprojects and Risk) conference at Nordic Hilton Hotel Reykjavik, 20 October 2022, Reykjavik, Iceland.
9. Title: **WtE preliminary project in Iceland - Assessing and dealing with different facets of risk** [151].
Author: Svana Helen Björnsdóttir
Presented at the IMaR 2024 conference at Nordica Hilton Reykjavik, 18 April 2024, Reykjavik, Iceland.

4.6.2 Master theses

Here is a list of Master Theses that were conducted as a part this thesis work.

1. Title: **Application of system safety to design and construction of a hydropower station** [152].
Author: Katrín Dögg Sigurðardóttir
Supervisors: Svana Helen Björnsdóttir and professor Páll Jensson.
Thesis of 30 ECTS credits for Master of Science in Engineering Management, Reykjavik University, June 2016.
Conference poster: Application of system safety to design and construction of a hydropower station, presented at the 4th European STAMP/STPA Workshop and Conference at ZHAW, 13-15 September 2016, Zürich, Switzerland [153].

2. Title: **Comparison of the application of risk management to medical devices guided by ISO 14971 and STAMP** [154].
Author: Helga Einarsdóttir
Supervisors: Svana Helen Björnsdóttir, Páll Jensson and Rögnvaldur J. Sæmundsson.
Thesis of 30 ECTS credits for Master of Science in Engineering Management, Reykjavik University, June 2017.
3. Title: **Risk Management in Almenni Collective Pension Fund.**
Author: Birgir Rafn Gunnarsson
Supervisors: Haraldur Óskar Haraldsson and Svana Helen Björnsdóttir.
Thesis of 30 ECTS credits for Master of Science in Financial Engineering, Reykjavik University, May 2012.
4. Title: **Supply Chain Risk Assessment** [155].
Author: Þórhallur Jóhannsson
Supervisors: Páll Jensson and Svana Helen Björnsdóttir.
Thesis of 30 ECTS credits for Master of Science in Engineering Management, Reykjavik University, May 2015.
5. Title: **Risk management and value creation - An international high-tech manufacturing company's approach to risk management and value creation in new product development projects** [156].
Author: Eyjólfur Alexandersson
Supervisor: Svana Helen Björnsdóttir
Thesis of 9 ECTS credits for Master of Project Management, Reykjavik University, May 2023.

4.6.3 Development of the STPA software tool

The STPA software tool was a spin-off of the Ph.D. thesis, an opportunity to create a STPA tool that supports STAMP/STPA work in the case studies conducted in the thesis. It was a 3-year Eureka-Eurostars funded project, a collaboration between Stiki and ZHAW. The author of this thesis was the project manager. The name of the project is: “E10663 – EERMF Enhanced Enterprise Risk Management Framework based on STPA”.

The purpose of the project was to create an Enhanced Enterprise Risk Management Framework (EERMF) that enables identification and assessment of hazards and risks using the STPA technique, detecting risks that are otherwise undetected within an organization. The purpose was furthermore to deliver a unique software solution that allows enterprises effectively to use STPA in a new risk management framework, enabling efficient risk identification and management of organizational and technical systems. By adopting a functional system view, STPA provides complete analysis of today's sociotechnical systems. The unique approach to embed STPA into an enhanced risk management framework enables a holistic assessment and management of risk.

The project proposal states that: “The goal is to develop an intelligent software application for applying the STPA hazard identification and risk analysis method to enterprise risk management. As an analysis method, STPA satisfies only part of necessary risk management activities but integrating it into a proven enterprise risk management framework, we create a complete, breakthrough solution for risk management. The enhanced enterprise risk management framework (EERMF) is generated from the research and experience of the consortium [...] over the past 22 years and applies to both procedural and technical aspects of systems, providing detailed hazard, safety, and security risks analysis”.

STPA specifically investigates risks generated by functional interaction between control-units present in a system, while safety and security are treated as an emergent system property. A safe and secure system operation can be achieved and maintained only when the system applies appropriate constraints that the system abides by. As a result, STPA is especially suitable for analysis of complex, dynamic, sociotechnical systems common today in most business sectors.

The EERMF will have two prototypes and a stand-alone software application for the STPA method, and a finished product complete with the entire risk management life cycle: identification, assessment, mitigation and prevention.”

A conference poster was created to explain the project [157]. The project started in 2016 and ended in 2019. The software is currently marketed and sold by Stiki under the brand name of Risk Management Studio [148], [158].

5 Discussion

In this chapter, research questions are answered individually. The scientific contribution and the limitations of this research are also discussed.

5.1 General risk analysis methodology

Research question 1: To what extent is it possible to formulate a general risk analysis methodology that can be used in many different disciplines?

It has been the purpose of all this thesis work to investigate different facets of risk analysis methodologies and techniques. All articles touch on the subject, but from a different perspective, for the purpose of getting a good understanding and knowledge of the subject as well as its limitations. The starting point of this thesis is risk management in organizations that use ISO standards for guidance when establishing their risk management system. From the beginning of the thesis, in the literature review, it became clear that risk terminology varies. It varies in the standards, and it varies in industry depending on the industry sector and culture.

In Article A, international standards are used to get a picture of the guidelines they give on risk management and risk analysis, and at the same time, the scientific basis of the standards is examined. In Article B, benchmarking theory is used to assess the quality of guidance for individual parts of risk management. Accredited certifications may give organizations a false sense of safety and security, as certification audits heavily depend on compliance factors. In Article C, a systems-theoretic method of risk analysis is applied to a project that is both complex and large and tests the risk analysis technique to identify the most important risk factor(s) to focus on at a given point in time. The approach applied originates in engineering and covers controllable system risk, with proper design and operation. The method does not include external factors, e.g., economic fluctuations and inflation. To get a better understanding of these systems' external risk factors, the thesis scope was extended and the VUCA method was investigated for comparison in Article E. The same project was chosen for this investigation both in Article C and E.

To get a deeper understanding of how STAMP, STPA and STECA are conducted and to create a supporting software tool, a STPA software development project was undertaken [159]⁵. It was a 3-year Eurostars funded project that resulted in a STPA software tool that has been used for most of the STAMP modeling and STPA and STECA work in this thesis. The design challenges are presented in Article D. This spin-off STPA software project forced clarification of abstraction of hierarchical control structures, distinction between a model and diagrams, and defining rule sets when developing and using software tools for support of the analysis work.

When examining the results of all articles, it becomes clear that risk management is a broad field that cuts across other disciplines and industries. Risk analysis is, however, a special field of study where research is carried out on the fundamental aspects of risk. Within that academic field, analysis of risk is defined in such a way that it includes risk assessment and risk treatment, contrary to definitions in ISO standards.

⁵ <https://www.riskmanagementstudio.com/stpa-software-solution/>

The main thing that limits organizations in adopting new risk analysis methods is that it involves acquiring new knowledge, learning new methods/techniques, and changing already existing processes and procedures. This comes at a cost, at least to begin with. In the case studies conducted in six different organizations, it was found that the will to improve and do better is present, but the benefits do not seem clear enough and the value of risk analysis and risk management is not sufficiently visible. However, it was shown that in mature risk management systems where the procedures are clear and the awareness of employees is high, the ability to change and adopt more effective risk analysis methods is already present.

Results also show that it is difficult to develop a universal risk management standard. The criteria and requirements of such a “golden standard” must be sufficiently general and universal to be useful to most people and organizations. At the same time, there is a need for guidelines for specific subjects with references that make it easier for users to find methods/techniques to analyze risk that are suitable for them. One must be careful not to have too much faith in certified risk management systems because it can lead to a false sense of safety and security.

The six case studies that were carried out show that all organizations have developed their own risk analysis technique, most of them rather simple and limited. No organization has a management system that cannot be improved to find risk factors that exist but could not be detected with current methods. The organizations differ and, in some cases, there is a risk associated with external factors and uncertainty that they have little control over.

The STAMP accident causation model along with the derived analysis techniques STPA, STPA-Sec and STECA go a long way in identifying hazards, threats and risk [6], [11], [160], [15]. The results of this thesis show that this methodology and analysis techniques can be used successfully in addition to traditional methods to find both the cause of hazard, threat, and risk, and to identify important time factors regarding risk in complex systems. This is important in complex sociotechnical systems, and it is especially important in the preparation and design phase of such projects/systems. The aim here is to embed safety and security in the system design from the beginning and so make it controllable regarding risk in the future. The results presented in Article C show that by applying STAMP as a methodology to develop a system model and the derived techniques, STPA and STECA, the most relevant risk factor(s) can be identified. It also supports finding ways (controls) to mitigate what has been found to be the main but not obvious risk in the preparation phase of the project/system.

The examination of VUCA [17] in Article E showed that the method offers a perspective on risk analysis that STAMP, STPA and STECA do not have. Both methods consider complexity, but with VUCA, volatility, uncertainty and ambiguity are examined separately.

The answer to research question 1 can be summarized as follows: It may be possible, but it is not practical to formulate a general risk analysis methodology that can be used in many different disciplines due to complexity and diversity of sectors and cultures. There is a contradiction in having a general and practical standard on risk management, and concurrently wanting it to give detailed guidance on appropriate methods and provide support on risk identification and analysis in complex human–system interaction. The same applies to general risk analysis methodology.

5.2 Guidance given in ISO standards on risk management

Research question 2: What guidance is given in ISO standards on risk management, especially for the critical step of risk analysis?

A variety of ISO standards were reviewed in the study reported in Article A, altogether 18 MSSs and guidelines based on the standards included in the annual ISO survey [19]. They all address risk management in some way. It is logical that some standards form the basis of risk management, which then other standards refer to and build on. An example of this is ISO Guide 73 [119] that defines risk management vocabulary, ISO 31000 [2] with general guidelines, and IEC 31010 [79] with risk assessment techniques. It is hardly realistic to expect that one “golden standard” for risk management can be created. However, for the standards to be of more help to users, risk terminology should be uniform and consistent in all standards because most organizations use not only one but many ISO standards. When the risk terminology is different, it can cause confusion. The guidance must be appropriate, and reference must be made to literature to help users find the necessary additional information. To achieve this, the development of ISO standards related to risk management must be based on interdisciplinary collaboration.

A literature review has revealed that complex sociotechnical systems require new risk analysis methods and techniques, for example, applying systems theory [161] in risk models. It would be helpful for users to have some guidance on these risk issues. ISO standards also need to follow the advancement of technology and societal changes, and they need to address the challenges of modern sociotechnical systems, for example, regarding automation and use of artificial intelligence. The guidance of ISO standards needs to guide users in the right direction in finding solutions and looking for additional knowledge when needed. If the standards are inappropriate, they will not achieve their aim to protect society from harm.

There is a contradiction in having a general and practical standard on risk management, and concurrently wanting it to give detailed guidance on appropriate methods and provide support on risk identification and analysis in complex human system interaction. ISO 31000 only addresses this kind of risk indirectly by emphasizing the importance of identifying risk and saying that it is important to consider factors like magnitude of risk, complexity, and connectivity. The additional guidance in IEC 31010, with an overview of several risk assessment techniques, fills in some of the gaps. Still missing though is the guidance to help identify and understand the complex interactions and emergent behavior that is inherent in present-day sociotechnical systems. None of the ISO standards reviewed in this article are adequate when it comes to managing risk and capturing complex risk concepts in the risk science field. This cannot be expected since standards are based on models of reality that can never fully incorporate all the complexity of real conditions.

The answer to research question 2 can be summarized as follows: Insufficient guidance is given in ISO standards on risk management, especially for the critical step of risk analysis. In many standards there is no guidance at all.

5.3 Alignment of ISO Standards with scientific literature on risk management

Research question 3: How well-aligned are ISO standards with state-of-the-art risk management literature?

Recent literature on risk management describes various risk issues and challenges faced when managing risk in complex sociotechnical systems. Several approaches to systems thinking have been proposed to understand such systems. These approaches may increase system and risk understanding but may still need to be supplemented with other approaches to adequately support risk management. Better modeling is advocated and qualitative modeling tools with description of systemic behavior are recommended for identification of possible accidents in complex systems. The ISO standards neither address the importance of risk models nor describe how to go about creating such models.

The literature reviewed in Article A confirms the importance of conducting a solid risk analysis in complex sociotechnical systems. This requires more knowledge of risk analysis than can be found in ISO standards. In fact, it requires both expertise in systems functionality and risk analysis methods. It is not within the reach of all companies to hire experts in risk analysis. Therefore, many projects and solutions can be expected to be brought to the market without adequate design, which creates unknown risk that can be difficult to manage. ISO's goal is to produce globally relevant international standards. ISO's strategy is: "ensuring a coherent and credible collection of standards that are used effectively by industry and bring recognized benefits to economies" and "identifying and meeting the changing needs of customers, with a focus on how they would like to use and access ISO standards" [162]. Four trends will impact ISO's future strategy: increasing trade uncertainty, changing societal expectations, urgency for sustainability, and digital transformation [163]. Therefore, the emphasis on effective use of standards as well as identification and meeting changing business needs is clear. The quality of standards must be measured against how well they align with scientific literature and state-of-the-art technology. It is a challenge to find one (golden) standard approach to model complex systems and identify their potential risk. It creates tension; complexity makes guidance more desirable, but overly prescriptive guidance may not be flexible enough to accommodate complexity. Over specifications of specific tasks that constitute compliance could even make systems more vulnerable to risk or unforeseen events. The study reported in Article A shows that the ISO standards on risk management are not based on risk science and not aligned with scientific literature. For effective risk management guidance, the ISO standards updating and alignment with the latest scientific literature on risk management is important. This is what industry needs, and this is furthermore ISO's strategic goal in coming years [163].

The answer to research question 3 can be summarized as follows: The ISO standards are not aligned with state-of-the-art risk management literature at all.

5.4 Risk analysis in practice

Research question 4: How is risk analysis conducted in real ISO certified organizations?

The six case studies that were conducted to analyze the real risk analysis practice show that risk analysis is done as a part of a documented risk assessment process and mostly following the risk management framework described in ISO 31000. There are differences according to organizational needs and business sectors and each organization has its own risk management culture. In no two cases was the risk analyzed in the same way. The techniques used are bottom-up and risk libraries are used to create an overview of risks. Risk

matrix with red, yellow and green colors are used to indicate high risk, medium risk and low risk factors. Risk is calculated as the multiple of likelihood, severity and sometimes also vulnerability. The scales are different, and the risk formulas differ. Only in one case was STAMP and STPA used parallel to traditional risk analysis with risk register and risk calculation for research purpose and to gather information and gain experience.

The answer to research question 4 can be summarized as follows: Risk analysis is in practice done with traditional a bottom-up techniques.

5.5 Development of a benchmarking model for risk management

Research question 5: Can a general benchmarking model for risk management be developed to evaluate the quality of a risk management process that is based on ISO MSS?

The results of Article B show that it can be difficult to assess the efficacy of risk management, even if the risk management system is ISO certified. Certification is not a guarantee of being able to identify and assess all relevant risk factors in business operations. Methods and tools are needed to support evaluation of the efficacy and robustness of a risk management system. The two-step benchmarking model developed as part of this thesis and presented in Article B can be used as a tool for this purpose and leaves opportunities for further development. The model uses an assessment template with a simple scoring system to verify and evaluate all main parts of risk management systems based on ISO 31000 [2]. If the evaluation is positive and the risk management system proves to have all necessary parts in it, the next step is to dive deeper and assess the efficacy of individual parts of the system. Risk analysis and risk assessment are two of the most challenging parts for many organizations (based on ISO 31000). These parts need to be examined and evaluated regarding the ability to detect risk, often in complex systems. In this study, the participants assessed their own risk management systems through a questionnaire. The answers were supported by documents of various kinds. After reviewing the answers and documents, interviews were conducted as audit meetings in line with ISO 19011 to verify all information provided [71]. Step 2 in the benchmarking model was applied to capture qualitative data. The scoring was in the form of “risk issues found”.

The study shows that it is important to build the benchmarks on risk science. Further research is needed to find out whether it is possible to develop a standardized scoring system based on risk science that serves as a good indicator of evaluation ability. There are also other aspects of risk management that need to be considered, for example, identification of risk leading indicators. Recent research has been conducted in this area [50]. The overall efficacy of the risk management system needs to be further examined. To handle complexity, robustness and resilience must also be addressed. More such factors need to be analyzed and ways found to measure and evaluate them.

Recent literature on risk management describes the importance of benchmarking models for improvements and quality assurance. The literature also describes various risk issues and challenges faced when managing risk in complex sociotechnical systems. Several approaches to systems thinking have been proposed to understand such systems. These approaches may increase system and risk understanding but may still need to be supplemented with other approaches to adequately support risk management. Better modeling is advocated and qualitative modeling tools with description of systemic behavior are recommended for identification and evaluation of risk in complex systems. ISO 31000 neither addresses the importance of risk models nor describes how to go about creating such models.

The answer to research question 5 can be summarized as follows: A two-step general benchmarking model for risk management was developed as part of this thesis to evaluate the quality of risk management processes that are based on ISO management system standards.

5.6 Application of a benchmarking model for evaluation of ISO risk management systems

Research question 6: How useful is a benchmarking model for risk management in terms of finding hidden risk issues and improvement opportunities?

The results presented in Article B show that ISO standards can be applied in many ways in risk management systems, depending on the nature of the operation and the business needs. Evidence, results, and testimonials presented in the article confirm that risk management is increasingly important for business, and it is becoming an integrated part of a management system. This is in line with findings in a former study, presented in Article A. The study presented in Article B also shows that in all six cases examined, different approaches are taken to risk analysis and risk management. By applying the benchmarking model developed in this study, it was possible to find both risk issues and risk factors that had not previously been found.

Table 12 in chapter 4 gives an overview of the risk issues found and shows in which organizations. The content of the table can be summarized as follows:

- Scope and outer boundary issues were found in 2 out of 6 cases.
- Interface issues were found in 3 out of 6 cases.
- Hierarchical issues were found in 1 out of 6 cases.
- Resource issues were found in 2 out of 6 cases.
- Issues regarding risk analysis ability to capture complex systems and business operations were found in 4 out of 6 cases.
- Issues regarding risk assessment ability to capture risk evaluation were found in 4 out of 6 cases.
- Issues regarding setting of risk criteria were found in 4 out of 6 cases.
- Issues regarding residual risk were found in 4 out of 6 cases.

Risk issues were identified in four out of six risk management systems. In the other two risk management systems, risk issues could not be completely verified (still marked as “No issues found”), which does not mean that risk issues did not exist at some point. Review of these findings with correspondence to the risk management description in ISO 31000:2018, presented in Table 12, shows that there is weakness in the risk management principles, the framework, and the process, Figure 2. In view of the previous study, this is a clear indication of a lack of guidance on risk management and inconsistency in risk terminology in ISO standards, as demonstrated in Table 4 and in Article B.

Testimonials confirm that all the organizations are searching for better and more efficient risk analysis methods; a systematic method that provides better risk finding assurance. Common causes for risk factors are often not identified because of border and interface issues, complexity issues, and lack of overview. One of the reasons is the frequently used bottom-up approach in risk assessments, where different departments assess their own risk and then risk information is compiled into one risk register (risk library) without further risk analysis. Emergent behavior, time lags, and relevant control or feedback loops are not identified through the risk management approach in any of the cases.

The risk management systems of the construction company (organization C) and the manufacturing company (organization D) proved to be satisfactory for the two projects analyzed in this study, a construction of one infrastructure facility and the development of one medical device. Despite being very different, both management systems are mature and based on many years of experience. During the construction phase of the construction facility, no guidance from ISO standards was used. The manufacturer of medical devices developed a risk management system for the development of medical devices that uses ISO standards as a basis, but the risk analysis technique was developed by risk experts within the company, where experience and knowledge of the design and production of medical devices has a long history. The manufacturer of medical devices tries to capture risk related to user errors of the medical device. The software company (organization E) is the only case where systems theory has been applied, but only for a short time. It is still being tested but the company has managed to improve its identification and analysis of risk with help of the STPA technique [11], [6].

Although not specifically analyzed, it is obvious that the organizations in this study have invested significantly in their risk management systems. Once an accredited certification has been obtained, there is increased reputational and image risk involved in losing or giving up the certification. The support from top management is essential, not only to establish the risk management system, but also to maintain it. It is understandable that people want to keep risk analysis as simple as possible. If a simple analysis has been done and it has been helpful, there is a reluctance to increase complexity, especially at increased cost. When is it necessary to take the next step? The decision is easier if a simpler and more cost-effective new method is found. Even then, regulatory requirements must be fulfilled.

During the time of the study (2014–2019) efforts to improve risk analysis were evident by the public supply system (organization B), the software company (organization E), and the pension fund (organization F). However, unsubstantiated methods are used, such as two-dimensional risk matrices, by all organizations except the software company. That company has been certified to ISO/IEC 27001 since 2004 and specialization in the risk field has driven knowledge and led to maturity of its risk management process which nevertheless has risk issues. All interviewees in this study noted that risk assessment, including risk analysis, has been a demanding and difficult task for them. Communicating results from risk assessments to either internal parties (e.g., board of directors) or external parties (e.g., governmental authorities), is also challenging. It was argued that especially third-party organizations (e.g., regulators, contractors, suppliers) did not always understand the effort associated with risk management. It was also argued that these parties lack an understanding of the complexity of risk management and the time and cost involved. This again increases risk.

The answer to research question 6 can be summarized as follows: The benchmarking model for risk management developed in this study proved useful in terms of finding hidden risk issues and improvement opportunities. It is a general model that can be used to assess the efficacy of individual parts of any risk management systems that is based on the ISO 31000 guidelines. By applying the benchmarks, it is possible to assess the efficacy of risk analysis and risk assessment, which are two of the most challenging parts of the risk management process for many organizations, and thus support the risk analysis method being used to identify risk.

5.7 Application of STAMP and STPA

Research question 7: Can STAMP and STPA analysis technique be applied to identify hazards, threats and risks that have not been previously found?

The purpose of this question is based on the need for better risk analysis methodologies and techniques to be able to capture risk in present-day complex systems. Systems that are sociotechnical systems, show emergent behavior, and have non-linear causal relations. Traditional analysis techniques are rooted in the discipline of project management. They are based on a bottom-up approach, as shown in all the case studies in this thesis work. The scientific literature, however, clearly demonstrates that new methods and techniques are needed to capture risk in such systems. Systems that have not been designed with regard to safety and security may store hidden risk that that is difficult to manage.

Scientific articles on STAMP and STPA show good results of using this method to detect hazards and threats in systems that have already been created and are already in use. The results indicate that through identification of hazards and threats risks can be found in such systems that have not been detected before. This is based both on the STAMP model that is used for analysis and the STPA technique, which uses a top-down approach to analyze accidents and losses which is important to prevent.

Going through this work with the organizational experts in the case studies, difficulties emerged. Since this is a teamwork, it is important for the experts to have some basic understanding of STAMP and STPA, which they did not have. It can also be sensitive to publish risk information that may point to a weakness in a system or operation. This work, however, started well this work still and a lot of data was collected and analyzes were made which were partially published in master theses and conference presentations which are listed in Section 4.6.

The answer to research question 7 can be summarized as follows: With STAMP and STPA it is possible to identify hazards, threats and risks that have not previously been found.

5.8 STAMP, STPA and STECA applied to achieve a safety and security-based design

Research question 8: Can the STAMP, STPA and STECA analysis techniques be applied to create a system model that can then be used to confirm a major national infrastructure concept? Can the model and the analysis techniques furthermore be used to identify and analyze project risk, and define requirements regarding risk mitigation from the early phase of the project and in that way fulfill the requirements of the engineering concept SbD?

The purpose of applying STAMP, STPA and STECA is that it is likely, based on the scientific literature, to give valid results regarding risk factors in the project that was chosen for the research. The project is the construction of a large WtE incineration plant that would serve the needs of all of Iceland in the coming decades. Since no decision has been made about the project, no one "owns" it, and no one has an interest in hiding facts about risk. There are no confidentiality restrictions regarding the project at this stage.

The study presented in Article C shows that the STAMP, STECA and STPA risk analysis techniques can be used to define complex projects and to decide on the optimal sequence of work components with regard to the least and most manageable project risk factors. In this study, the subject is WtE incineration, which is an important sustainability project in any country. The decision-making process of the project discussed here is

complicated because it brings together different parties, both private and public, in a partnership that needs to be carefully analyzed to get an optimal structure. The partnership and all its prerequisites and criteria must be carefully thought out before the project begins. It must also be ensured that the legislation is sufficiently clear regarding tender requirements, possible competitive factors, material flow for incineration, the division of responsibilities between municipalities and all the other parties involved in the project.

There are two types of public bodies involved in the project, the local authorities, and the governmental authorities, with politically elected representatives which are replaced at different times. The project also includes private parties and investors who participate in the project after a decision has been made to go ahead with the project. Only then can the actual preparatory work for the project begin, e.g., design, bidding and contract making. In the case discussed here, it is likely that known solutions in combustion technology can be used. Less known is the technology of carbon capture and storage during operation.

This study shows that there is a need for a continuous and revised analysis of risk factors during the project life cycle. After the WtE incinerator has been built and daily operations start, regular risk analysis and risk assessment must be carried out continuously, but this will most likely follow a standard process and be part of the internal control and coordinated management system of quality, health, safety, security, and environmental factors. To ensure reliability and credibility, it may be wise to build the management system on international ISO standards and obtain accredited ISO certifications for the entire operation.

It is not a coincidence that all ISO management standards now require risk analysis as a part of decision making and good governance. The standards, however, do not give much guidance on how to conduct risk analysis. This study shows that the STAMP, STECA and STPA techniques are effective when preparing large and complex projects that may take years to complete, like a WtE project. It helps to organize the project in an optimal way, also considering time factors. It supports decision making regarding when and how is best to take every step in the project. By identifying risk factors in time, it is possible to find ways to mitigate risk and make it manageable. This study confirms results from Bjerga et al. [107] as being suitable approaches to analyze risk in complex systems, with focus on the treatment of uncertainty and potential surprises linked to the operation of complex systems.

This study also reveals the great responsibility government, and municipalities have regarding projects like this one, to make sure that there is an administration that ensures the right channel for preparation and all decisions. The law is not clear enough in this regard and this must therefore be considered a weakness – or risk. One way to mitigate this risk would be to enact a special law on the project. This has been done in the past for the development of important national infrastructure.

The answer to research question 8 can be summarized as follows: With STAMP, STPA and STECA it was possible to create a system model of the WtE project in an iterative process. The model was reviewed by many experts in different fields to make sure that it is complete. The STAMP system model was then used as basis for analyzing all feedback and control actions, each stakeholder needs to do his job and be responsible. STPA sets the framework for the risk analysis, but with STECA it is possible to organize the model (in a hierarchical way if needed) and identify risk factors at an early stage before the project starts. In that way the project concept could be confirmed and one major, but not obvious risk factor could be identified that needs to be addressed before the project starts.

5.9 Use of multiple control structures during system modeling with STAMP

Research question 9: Can the concept of control structures in STAMP be developed to capture the use of multiple diagrams to represent one model?

STAMP is usually represented as a single control structure diagram, normally as a hierarchical control structure showing interactions needed to ensure safety and security within the system. The modeling work is iterative. It typically starts at a rather abstract level but is then refined during the modeling or at later stages in the analysis process. Usually, no differentiation is made between the control structure model and its representation as a diagram. The concept of using multiple diagrams to represent one model of the control structure makes it possible for the analyst to study individual system elements and their interactions at various levels. To ensure the completeness of the analysis it is necessary to have solid rulesets. There are also consistency issues to be considered, e.g., that the control structure representations are consistent with the model and with each other.

The answer to research question 9 can be summarized as follows: The concept of control structures in STAMP can be developed to capture the use of multiple diagrams to represent one model. The rulesets must however be further developed and tested, and the consistency between the rulesets and the model depiction, diagrams, must be checked and ensured.

5.10 Application of the VUCA meter

Research question 10: Can the VUCA meter augment the traditional project risk identification process?

The VUCA meter provides a normative approach to identify risk in projects that includes complexity, uncertainty, volatility, and ambiguity. The study clearly indicates that the VUCA meter can be developed to be a significant addition to the conventional risk identification process for large projects that are at an early stage.

The answer to research question 10 can be summarized as follows: The VUCA meter facilitates a discussion that gets people to think beyond the traditional framework for identifying project risk factors. Consequently, the so called “fat tail” events that are not apprehended with the conventional analysis technique, are captured by the VUCA meter.

6 Conclusions and Future Work

This chapter summarizes the results, states the conclusions, and outlines the direction of future work.

6.1 Conclusions

This Ph.D. thesis focuses on risk management, especially risk analysis, in business life and how risk analysis can be conducted in an optimal way to identify hidden risk. It is important to choose a good methodology and technique, but ISO standards do not give much guidance regarding how to conduct such risk analysis. The ISO standards, however, provide a description of a risk management framework that helps many organizations to establish their management system. It is important to be able to assess the efficacy of such a system and the whole risk management process to minimize the risk of experiencing false safety and security.

Despite all the rhetoric and money invested in risk management, businesses too often treat it as merely a compliance issue. Risk management is implemented by setting rules and making sure that all employees follow them. Many such rules do make sense and may reduce harmful risk, but rules-based risk management will not diminish the likelihood or the impact of a disaster [4]. Accredited certification is a way for managers to ensure that all business functions are carried out according to proper processes and procedures, potentially reducing risk. However, this approach does not accommodate the complexity of sociotechnical systems, emergent behavior, and nonlinear causal relations. Thus, better guidelines are required for analyzing and managing risk than those provided in the current ISO standards.

It is hardly realistic to expect that one “golden standard” for risk management can be created. However, for the standards to be of more help to users, risk terminology should be uniform and consistent in all standards because most organizations use not only one but many ISO standards. When the risk terminology is different, it can cause confusion. The guidance must be appropriate, and reference must be made to literature to help users find the necessary additional information. To achieve this, the development of ISO standards related to risk management must be based on interdisciplinary collaboration.

The **first research question** identified the latest developments in ISO management standards, i.e., the importance of risk management all standards. It demonstrated the dissemination of the standards and the importance of accredited certification for businesses. The investigation of the standards revealed that the standards do not have a clear and uniform definition of risk terms and their risk terminology is not aligned with the scientific literature. The standards approach does not accommodate the complexity of sociotechnical systems, emergent behavior, and nonlinear causal relations. It is logical that some standards form the basis of risk management, which then other standards refer to and build on. It is hardly realistic to expect that one “golden standard” for risk management can be created. However, for the standards to be of more help to users, risk terminology should be uniform and consistent in all standards because most organizations use not only one but many ISO standards.

The **second research question** focused on what guidance is given on key elements of risk management in all ISO MSS included in the annual ISO survey and the guidelines they refer to regarding risk, altogether eighteen ISO standards. By investigating the development over eight years it was possible to see their increased emphasis on risk management and risk analysis, and their spread and development in the number of accredited certificates. The investigation furthermore revealed that little guidance is given on how to conduct risk analysis and what analysis methods to use. There is no reference to risk science literature in the ISO standards.

The **third research question** focused on how well-aligned the ISO standards with the scientific literature and state-of-the-art thinking on risk. It is interrelated with the previous research question. It reveals that the ISO standards are not aligned with state-of-the-art risk management literature. Neither are risk terms aligned with the risk science literature, nor is there consistency between individual standards in the risk terminology and guidelines. The standards neither reflect collaboration with academic organizations nor experts in risk science. This means that the ISO standards may not be appropriate for the management of risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems.

The **fourth research question** focused on how risk analysis is conducted in real ISO certified organizations. Six case studies were conducted, where the risk analysis process in six different ISO certified organizations, operating in different business sectors, were analyzed. The case studies reveal that traditional analysis techniques are applied, e.g., risk matrix and calculation of risk as a multiple of likelihood, severity and sometimes vulnerability. In one case STAMP and STPA has been used alongside conventional methods.

The **fifth research question** focused on how risk ISO management systems can be assessed and audited, and their quality evaluated with the aim to confirm their efficacy, find hidden risk factors and improvement opportunities. Based on the risk management framework described in ISO 31000 and combining risk science with benchmarking theory it was possible to develop a two-step benchmarking model. The model was applied and tested in case studies with six real-life ISO certified organizations using traditional analysis techniques. The benchmarking model proved useful in all cases. It provides rigor when assessing and evaluating the efficacy of an ISO risk management system.

The **sixth research question** focused on the usefulness of the benchmarking model in finding hidden risk issues and improvement opportunities. The application of the benchmarking model in the previously mentioned case studies revealed that despite well-established ISO certified management systems it is possible to find hidden risk issues and risk factors that had not previously been identified.

The **seventh research question** focused on the capability of STAMP and STPA to identify hazards, threats and risks that have not been previously found in the six ISO certified organizations? This requires teamwork with experts in the organizations. None of the experts had experience with STAMP/STPA. Nevertheless, the work started well, and several conference presentations were given on the results. Once a scientific paper had been drafted, it proved not possible to make the results public without risking breach of confidentiality.

The **eighth research question** focused on the application and usefulness of STAMP, STPA and STECA in creating a system model that can then be used to confirm a major national infrastructure project concept. Through iterative work a system model was developed and by also applying stakeholder theory it was possible to identify and align actors and stakeholders in the model. The model was confirmed through a review process

where many stakeholder representatives confirmed their role and responsibilities, their need for information and feedback, and their control actions. This way it is possible to solve the objectives of a safety and security-based design of a major national infrastructure.

The **ninth research question** focused on the concept of control structures in STAMP and if it can be developed to capture the use of multiple diagrams to represent one model. The investigation of the concept of multiple diagrams representing one and the same STAMP system model was done through a Eurostars funded software project. Rulesets for individual use cases were derived and a successful preliminary verification of them was conducted, but the consolidation of the rules must still be done. This is useful when it is necessary to dive deeper into the details of a system. It takes effort to comply with the ruleset and constraints. Through a software tool it should be possible to automate this functionality and therefore it should not have to mean substantial additional workload for the analyst. The ruleset and constraints allowing complementing views was successfully implemented in a STPA software tool and all the diagrams in Article D were created with this tool.

The **tenth research question** focused on the capabilities of the VUCA meter and if it can augment the traditional project risk identification process. The VUCA meter offers a normative approach to identify risk in projects that includes complexity, uncertainty, volatility, and ambiguity. This approach is different from STAMP, STPA and STECA and offers a different perspective on risk.

6.2 Future work

This Ph.D. thesis offers interesting future research opportunities regarding further development of standardization in risk management, to monitor the development of ISO standards, and promote their scientific basis. More specifically, this thesis offers opportunities to further investigate how the requirements of ISO management standards can be used to meet the requirements for safety and security in design. In particular, those that address analysis of hazards, threats and risk, risk assessment and risk management. Users aim is to successfully be able to design safety and security into their systems, supporting them in finding ways to mitigate risk and make complex systems controllable in terms of risk. Knowledge gained from case studies, both data collected and from interviews, can be used to further evaluate existing ISO management systems, the benchmarking model and evaluation of their efficacy. There is an opportunity to better align the standards with the risk science and to apply new analysis methodologies and techniques developed in the field of risk science.

Even though much time was spent on the case studies, it was not possible to introduce STAMP and STPA adequately to their participants. Each organization possesses knowledge and expertise that would have been interesting to analyze further based on STAMP and STPA, but it requires participants' basic understanding of STAMP and STPA. If the opportunity arises, it would be interesting to dive even deeper into these case studies and possibly improve the actual analysis technology in all the organizations. It would also be interesting to further develop the benchmarking model and test it further, especially in real ISO certified organizations.

Continuing testing STAMP and STPA, STPA-Sec and STECA as analysis techniques to achieve the SbD engineering concept in large infrastructure projects is of great interest and importance. Such projects tend to go over budget, time, and cost schedule. Here is a big opportunity and much to gain if stakeholders and actors can be involved in the early phase to participate and share knowledge and information regarding possible risk factors. The WtE project provides an opportunity to continue the research as the project progresses. The

documentation of the process until finished will provide interesting data for later research and analysis. In this respect it is worth mentioning that continuous analysis of stakeholders and the transfer of the WtE project from preparation phase with STECA to system design with STPA provides research opportunity. To further classify and even prioritize stakeholders is also of interest. Furthermore, to take the step to a more hierarchical control structure as the work continues.

There is interest in further developing and improving the functionality of the STPA software that has been used in the analysis work. Such software facilitates analytical work and can make it better understandable for analysts and those who make decisions based on the results of such analyses. It remains a future task to connect different diagrams graphically and make it possible for the analyst to easily move between control structure levels (zoom in and out) and dive into specific elements in a simple way for further analysis.

A variety of external, unexpected, and unforeseen factors can affect a system that has been specially designed with safety and security in mind. This thesis work also offers an interesting future research opportunities to further investigate risk factors in the WtE project with VUCA. The VUCA analysis technique considers external factors that cannot be directly controlled within a system. To combine STAMP, STPA and VUCA in the upcoming risk analysis in the WtE project is a research opportunity to investigate the different perspectives the analysis techniques provide, and thus create a clearer picture of risk.

References

- [1] “Cambridge Dictionary, risk management.” Accessed: Mar. 30, 2024. [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/risk-management>
- [2] International Organization for Standardization, “ISO 31000:2018, Risk management - Principles and guidelines.” ISO, Geneva, Switzerland, 2018.
- [3] “The Society for Risk Analysis - SRA.” Accessed: Jul. 13, 2020. [Online]. Available: <https://www.sra.org/about-society-risk-analysis>
- [4] R. S. Kaplan and A. Mikes, “Managing Risks: A New Framework,” *Harvard Business Review*. Accessed: Apr. 14, 2017. [Online]. Available: <https://hbr.org/2012/06/managing-risks-a-new-framework>
- [5] N. N. Taleb, *The Black Swan: Second Edition: The Impact of the Highly Improbable: With a new section: “On Robustness and Fragility,”* 2nd edition. New York: Random House Publishing Group, 2010.
- [6] N. G. Leveson, *Engineering a Safer World*. 2011. Accessed: Jul. 03, 2018. [Online]. Available: <https://mitpress.mit.edu/books/engineering-safer-world>
- [7] “Qualitative vs. Quantitative Data in Research: The Difference | Fullstory,” Qualitative vs. quantitative data in research: what’s the difference? Accessed: May 12, 2024. [Online]. Available: <https://www.fullstory.com/blog/qualitative-vs-quantitative-data/>
- [8] “Understanding the Difference Between Quantitative and Qualitative Analytics,” Michigan State University. Accessed: May 12, 2024. [Online]. Available: <https://www.michiganstateuniversityonline.com/resources/business-analytics/difference-between-quantitative-and-qualitative-analytics/>
- [9] “ISO - Copyright,” ISO. Accessed: May 05, 2024. [Online]. Available: <https://www.iso.org/copyright.html>
- [10] “ISO - Store,” ISO. Accessed: May 05, 2024. [Online]. Available: <https://www.iso.org/store.html>
- [11] N. Leveson, “A new accident model for engineering safer systems,” *Safety Science*, vol. 42, no. 4, pp. 237–270, Apr. 2004, doi: 10.1016/S0925-7535(03)00047-X.
- [12] N. G. Leveson, “Applying systems thinking to analyze and learn from events,” *Safety Science*, vol. 49, no. 1, pp. 55–64, Jan. 2011, doi: 10.1016/j.ssci.2009.12.021.
- [13] N. G. Leveson and J. P. Thomas, *STPA Handbook*. Leveson and Thomas, 2018. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- [14] W. Young and N. G. Leveson, “An integrated approach to safety and security based on systems theory,” *Commun. ACM*, vol. 57, no. 2, pp. 31–35, Feb. 2014, doi: 10.1145/2556938.
- [15] C. H. Fleming and N. G. Leveson, “Early Concept Development and Safety Analysis of Future Transportation Systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 12, pp. 3512–3523, Dec. 2016, doi: 10.1109/TITS.2016.2561409.
- [16] T. V. Fridgeirsson, H. T. Ingason, H. I. Jonasson, and B. H. Kristjansdottir, “The VUCAlity of Projects: A New Approach to Assess a Project Risk in a Complex World,” *Sustainability*, vol. 13, no. 7, Art. no. 7, Jan. 2021, doi: 10.3390/su13073808.
- [17] N. Bennett and G. J. Lemoine, “What VUCA Really Means for You,” *Harvard Business Review*, Jan. 01, 2014. Accessed: Jul. 27, 2023. [Online]. Available: <https://hbr.org/2014/01/what-vuca-really-means-for-you>
- [18] PMI, *Project Management Institute, The Standard for Risk Management in Portfolios, Programs, and Projects*. PMI, Newtown Square, PA, USA, 2019.
- [19] International Organization for Standardization, “The ISO Survey,” The ISO Survey. Accessed: Jul. 09, 2020. [Online]. Available: <https://www.iso.org/the-iso-survey.html>

- [20] S. H. Björnsdóttir, P. Jensson, R. J. de Boer, and S. E. Thorsteinsson, “The Importance of Risk Management: What is Missing in ISO Standards?,” *Risk Analysis*, vol. n/a, no. n/a, Sep. 2021, doi: 10.1111/risa.13803.
- [21] S. Talapatra, M. K. Uddin, and M. H. Rahman, “Development of an Implementation Framework for Integrated Management System Based on the Philosophy of Total Quality Management,” *American Journal of Industrial and Business Management*, vol. 08, no. 06, Art. no. 06, Jun. 2018, doi: 10.4236/ajibm.2018.86101.
- [22] S. Talapatra and Md. K. Uddin, “Prioritizing the barriers of TQM implementation from the perspective of garment sector in developing countries,” *Benchmarking: An International Journal*, vol. 26, no. 7, pp. 2205–2224, Jan. 2019, doi: 10.1108/BIJ-01-2019-0023.
- [23] F. Franceschini, M. Galetto, and P. Cecconi, “A worldwide analysis of ISO 9000 standard diffusion: Considerations and future development,” *Benchmarking: An International Journal*, vol. 13, no. 4, pp. 523–541, Jan. 2006, doi: 10.1108/14635770610676326.
- [24] G. C. Kölln, M. Klicker, and S. Schmidt, “Comparison of hazard analysis methods with regard to the series development of autonomous vehicles,” in *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, Oct. 2019, pp. 2969–2975. doi: 10.1109/ITSC.2019.8916932.
- [25] J. Moriarty and C. Smallman, “En Route to a Theory of Benchmarking,” *Benchmarking: An International Journal*, vol. 16, Jul. 2009, doi: 10.1108/14635770910972423.
- [26] M. M. Yasin, “The theory and practice of benchmarking: then and now,” *Benchmarking: An International Journal*, vol. 9, no. 3, pp. 217–243, Jan. 2002, doi: 10.1108/14635770210428992.
- [27] C. H. Fleming, “Systems-Theoretic Early Concept Analysis (and Development),” 4th STAMP Workshop at MIT, Mar. 23, 2015.
- [28] Parliament and Council of the European Union, “General Data Protection Regulation 2016/679 of the European Parliament and the Council.pdf,” EUR-Lex Access to European Union Law. Accessed: Mar. 14, 2017. [Online]. Available: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1489504512384&from=en>
- [29] “The Global Risks Report 2020,” The World Economic Forum, 2020. [Online]. Available: <https://www.weforum.org/reports/the-global-risks-report-2020/>
- [30] “The Global Risks Report 2021,” The World Economic Forum, 2021. [Online]. Available: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
- [31] “The Global Risks Report 2022,” The World Economic Forum, 2022. [Online]. Available: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
- [32] “The Global Risks Report 2023,” The World Economic Forum, 2023. [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
- [33] “COPOLCO.” Accessed: Feb. 15, 2021. [Online]. Available: https://www.iso.org/sites/ConsumersStandards/1_standards.html
- [34] T. Aven and M. Ylönen, “The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?,” *Reliability Engineering & System Safety*, vol. 189, pp. 279–286, Sep. 2019, doi: 10.1016/j.ress.2019.04.035.
- [35] International Organization for Standardization, “ISO 13485:2016, Medical devices - Quality management systems - Requirements for regulatory purposes.” ISO, Geneva, Switzerland, 2016.
- [36] International Organization for Standardization, “ISO 14971:2019, Medical devices - Application of risk management to medical devices.” ISO, Geneva, Switzerland, 2019. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html>
- [37] D. L. Alderson, G. G. Brown, and W. M. Carlyle, “Operational Models of Infrastructure Resilience,” *Risk Analysis*, vol. 35, no. 4, pp. 562–586, 2015, doi: 10.1111/risa.12333.
- [38] P. Carayon, P. Hancock, N. Leveson, I. Noy, L. Sznclwar, and G. van Hootegem, “Advancing a sociotechnical systems approach to workplace safety – developing the conceptual framework,” *Ergonomics*, vol. 58, no. 4, pp. 548–564, Apr. 2015, doi: 10.1080/00140139.2015.1015623.
- [39] B. A. Carreras, D. E. Newman, I. Dobson, V. E. Lynch, and P. Gradney, “Thresholds and Complex Dynamics of Interdependent Cascading Infrastructure Systems,” in *Networks of Networks: The Last Frontier of Complexity*, G. D’Agostino and A. Scala, Eds., in Understanding Complex Systems. , Cham: Springer International Publishing, 2014, pp. 95–114. doi: 10.1007/978-3-319-03518-5_5.

- [40] S. Dekker, P. Cilliers, and J.-H. Hofmeyr, “The complexity of failure: Implications of complexity theory for safety investigations,” *Safety Science*, vol. 49, no. 6, pp. 939–945, Jul. 2011, doi: 10.1016/j.ssci.2011.01.008.
- [41] Y. Holovatch, R. Kenna, and S. Thurner, “Complex systems: physics beyond physics,” *Eur. J. Phys.*, vol. 38, no. 2, p. 023002, Feb. 2017, doi: 10.1088/1361-6404/aa5a87.
- [42] J. Rasmussen, “Risk management in a dynamic society: a modelling problem,” *Safety Science*, vol. 27, no. 2–3, pp. 183–213, Nov. 1997, doi: 10.1016/S0925-7535(97)00052-0.
- [43] E. Zio, “Challenges in the vulnerability and risk analysis of critical infrastructures,” *Reliability Engineering & System Safety*, vol. 152, pp. 137–150, Aug. 2016, doi: 10.1016/j.ress.2016.02.009.
- [44] T. Aven, “The Call for a Shift from Risk to Resilience: What Does it Mean?,” *Risk Analysis*, vol. 39, no. 6, pp. 1196–1203, 2019, doi: 10.1111/risa.13247.
- [45] G. Montibeller and D. von Winterfeldt, “Cognitive and Motivational Biases in Decision and Risk Analysis,” *Risk Analysis*, vol. 35, no. 7, pp. 1230–1251, 2015, doi: 10.1111/risa.12360.
- [46] E. J. Oughton *et al.*, “A Risk Assessment Framework for the Socioeconomic Impacts of Electricity Transmission Infrastructure Failure Due to Space Weather: An Application to the United Kingdom,” *Risk Analysis*, vol. 39, no. 5, pp. 1022–1043, 2019, doi: 10.1111/risa.13229.
- [47] D. J. Rozell, “The Ethical Foundations of Risk Analysis,” *Risk Analysis*, vol. 38, no. 8, pp. 1529–1533, 2018, doi: 10.1111/risa.12971.
- [48] T. Aven and E. Zio, “Foundational Issues in Risk Assessment and Risk Management,” *Risk Analysis*, vol. 34, no. 7, pp. 1164–1172, 2014, doi: 10.1111/risa.12132.
- [49] Ø. Amundrud, T. Aven, and R. Flage, “How the definition of security risk can be made compatible with safety definitions,” *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 231, no. 3, pp. 286–294, Jun. 2017, doi: 10.1177/1748006X17699145.
- [50] N. Leveson, “A systems approach to risk management through leading safety indicators,” *Reliability Engineering & System Safety*, vol. 136, pp. 17–34, Apr. 2015, doi: 10.1016/j.ress.2014.10.008.
- [51] T. Aven, “On the new ISO guide on risk management terminology,” *Reliability Engineering & System Safety*, vol. 96, no. 7, pp. 719–726, Jul. 2011, doi: 10.1016/j.ress.2010.12.020.
- [52] B. Barafort, A.-L. Mesquida, and A. Mas, “Integrating risk management in IT settings from ISO standards and management systems perspectives,” *Computer Standards & Interfaces*, vol. 54, pp. 176–185, Nov. 2017, doi: 10.1016/j.csi.2016.11.010.
- [53] Leitch M., “ISO 31000 2009 The New Intl Standard on Risk Mgmt.pdf.” *Risk Analysis Journal*, Vol. 30, No. 6, 2010, Apr. 08, 2010. Accessed: Apr. 02, 2017. [Online]. Available: <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2010.01397.x/full>
- [54] Olechowski A., Oehmen J., Seering W., and Ben-Daya M., “The Professionalization of Risk Management.pdf.” *International Journal of Project Management*, Sep. 04, 2016. Accessed: Feb. 04, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0263786316300631>
- [55] G. Purdy G., “ISO 31000:2009—Setting a New Standard for Risk Management,” *Risk Analysis*, vol. 30, no. 6, pp. 881–886, Jun. 2010, doi: 10.1111/j.1539-6924.2010.01442.x.
- [56] T. Parviainen, F. Goerlandt, I. Helle, P. Haapasaaari, and S. Kuikka, “Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions,” *Journal of Environmental Management*, vol. 278, p. 111520, Jan. 2021, doi: 10.1016/j.jenvman.2020.111520.
- [57] G. H. Silva Rampini, H. Takia, and F. T. Bessaneti, “Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes,” *Procedia Manufacturing*, vol. 39, pp. 894–903, Jan. 2019, doi: 10.1016/j.promfg.2020.01.400.
- [58] “Cambridge Dictionary, benchmarking.” Accessed: Mar. 30, 2024. [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/benchmarking>
- [59] N. Herbst *et al.*, “Quantifying Cloud Performance and Dependability: Taxonomy, Metric Design, and Emerging Challenges,” *ACM Trans. Model. Perform. Eval. Comput. Syst.*, vol. 3, no. 4, p. 19:1-19:36, Aug. 2018, doi: 10.1145/3236332.

- [60] S. Kounev, K.-D. Lange, and J. von Kistowski, *Systems Benchmarking: For Scientists and Engineers*. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-41705-5.
- [61] T. O. Olawumi and D. W. M. Chan, "Development of a benchmarking model for BIM implementation in developing countries," *Benchmarking: An International Journal*, vol. 26, no. 4, pp. 1210–1232, Jan. 2019, doi: 10.1108/BIJ-05-2018-0138.
- [62] T. J. M. van der Voordt and P. A. Jensen, "Measurement and benchmarking of workplace performance: Key issues in value adding management," *Journal of Corporate Real Estate*, vol. 20, no. 3, pp. 177–195, Jan. 2018, doi: 10.1108/JCRE-10-2017-0032.
- [63] R. D. Staiger, H. Schwandt, M. A. Puhan, and P.-A. Clavien, "Improving surgical outcomes through benchmarking," *British Journal of Surgery*, vol. 106, no. 1, pp. 59–64, Jan. 2019, doi: 10.1002/bjs.10976.
- [64] S. K. Mangla, S. Luthra, and S. Jakhar, "Benchmarking the risk assessment in green supply chain using fuzzy approach to FMEA: Insights from an Indian case study," *Benchmarking: An International Journal*, vol. 25, no. 8, pp. 2660–2687, Jan. 2018, doi: 10.1108/BIJ-04-2017-0074.
- [65] P. Hoffmann, H. Schiele, and K. Krabbendam, "Uncertainty, supply risk management and their impact on performance," *Journal of Purchasing and Supply Management*, vol. 19, no. 3, pp. 199–211, Sep. 2013, doi: 10.1016/j.pursup.2013.06.002.
- [66] B. H. MacGillivray, J. V. Sharp, J. E. Strutt, P. D. Hamilton, and S. J. T. Pollard, "Benchmarking Risk Management Within the International Water Utility Sector. Part II: A Survey of Eight Water Utilities," *Journal of Risk Research*, vol. 10, no. 1, pp. 105–123, Jan. 2007, doi: 10.1080/13669870601011191.
- [67] Hartono, E. Ongko, and D. Abdullah, "HFLTS-DEA Model for Benchmarking Qualitative Data," *Int. J. Advance Soft Compu. Appl.*, vol. 11, no. 2, pp. 109–131, Jul. 2019.
- [68] M. Björklund, "Benchmarking tool for improved corporate social responsibility in purchasing," *Benchmarking: An International Journal*, vol. 17, no. 3, pp. 340–362, Jan. 2010, doi: 10.1108/14635771011049335.
- [69] J. P. Moriarty and C. Smallman, "En route to a theory of benchmarking," *Benchmarking: An International Journal*, vol. 16, no. 4, pp. 484–503, Jan. 2009, doi: 10.1108/14635770910972423.
- [70] S. Talapatra and K. Uddin, "Understanding the difficulties of implementing TQM in garment sector: A case study of some RMG industries in Bangladesh," in *International Conference on Mechanical, Industrial and Materials Engineering 2017 (ICMIME2017)*, Rajshahi, Bangladesh: ICMIME2017, Dec. 2017, p. 6. Accessed: Nov. 01, 2022. [Online]. Available: <http://icmime-ruet.ac.bd/2017/DIR/Contents/Technical%20Papers/Industrial%20Engineering/IE-243.pdf>
- [71] International Organization for Standardization, "ISO 19011:2018, Guidelines for auditing management systems." IEC, Geneva, Switzerland, 2018. Accessed: Jul. 20, 2020. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/00/70017.html>
- [72] International Organization for Standardization, "ISO 9001:2015, Quality management systems - Requirements." ISO, Geneva, Switzerland, 2015.
- [73] International Organization for Standardization, "ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements." ISO, Geneva, Switzerland, 2013.
- [74] International Organization for Standardization, "ISO 45001:2018, Occupational health and safety management systems — Requirements with guidance for use." ISO, Geneva, Switzerland, 2018. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/37/63787.html>
- [75] International Organization for Standardization, "ISO 14001:2015, Environmental management systems - Requirements with guidance for use." ISO, Geneva, Switzerland, 2015.
- [76] S. Talapatra and K. Uddin, "Some obstacles that affect the TQM implementation in Bangladeshi RMG Sector: An empirical study," presented at the International Conference on Industrial Engineering and Operations Management 2018, Bandung, Indonesia: IEOM Society International, Mar. 2018, p. 13. [Online]. Available: <http://ieomsociety.org/ieom2018/papers/401.pdf>

- [77] A. Klinke and O. Renn, "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies¹," *Risk Analysis*, vol. 22, no. 6, pp. 1071–1094, 2002, doi: <https://doi.org/10.1111/1539-6924.00274>.
- [78] L. A. (Tony) Cox, "What's Wrong with Risk Matrices?," *Risk Analysis*, vol. 28, no. 2, pp. 497–512, 2008, doi: <https://doi.org/10.1111/j.1539-6924.2008.01030.x>.
- [79] The International Electrotechnical Commission, "IEC 31010:2019, Risk management - Risk assessment techniques." IEC, Geneva, Switzerland, 2019. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/21/72140.html>
- [80] International Organization for Standardization, "IEC 31010:2009, Risk management - Risk assessment techniques." IEC, Geneva, Switzerland, 2009.
- [81] R. Fellows and A. M. M. Liu, "Managing organizational interfaces in engineering construction projects: addressing fragmentation and boundary issues across multiple interfaces," *Construction Management and Economics*, vol. 30, no. 8, pp. 653–671, Aug. 2012, doi: 10.1080/01446193.2012.668199.
- [82] A. Mikes, "From counting risk to making risk count: Boundary-work in risk management," *Accounting, Organizations and Society*, vol. 36, no. 4, pp. 226–245, May 2011, doi: 10.1016/j.aos.2011.03.002.
- [83] V. Zerjav, "Design boundary dynamics in infrastructure projects: Issues of resource allocation, path dependency and problem-solving," *International Journal of Project Management*, vol. 33, no. 8, pp. 1768–1779, Nov. 2015, doi: 10.1016/j.ijproman.2015.09.009.
- [84] J. Lathrop and B. Ezell, "A systems approach to risk analysis validation for risk management," *Safety Science*, vol. 99, pp. 187–195, Nov. 2017, doi: 10.1016/j.ssci.2017.04.006.
- [85] C. Luo, Y. Ju, P. Dong, E. D. R. S. Gonzalez, and A. Wang, "Risk assessment for PPP waste-to-energy incineration plant projects in china based on hybrid weight methods and weighted multigranulation fuzzy rough sets," *Sustainable Cities and Society*, vol. 74, p. 103120, Nov. 2021, doi: 10.1016/j.scs.2021.103120.
- [86] Y. Wu, C. Xu, L. Li, Y. Wang, K. Chen, and R. Xu, "A risk assessment framework of PPP waste-to-energy incineration projects in China under 2-dimension linguistic environment," *Journal of Cleaner Production*, vol. 183, pp. 602–617, May 2018, doi: 10.1016/j.jclepro.2018.02.077.
- [87] C. Cui, C. Sun, Y. Liu, X. Jiang, and Q. Chen, "Determining critical risk factors affecting public-private partnership waste-to-energy incineration projects in China," *Energy Science & Engineering*, vol. 8, no. 4, pp. 1181–1193, 2020, doi: 10.1002/ese3.577.
- [88] L. Wang and X. Zhang, "Critical Risk Factors in PPP Waste-to-Energy Incineration Projects," *International Journal of Architecture, Engineering and Construction*, vol. 6, Jun. 2017, doi: 10.7492/IJAEC.2017.012.
- [89] Y. Xu, A. P. C. Chan, B. Xia, Q. K. Qian, Y. Liu, and Y. Peng, "Critical risk factors affecting the implementation of PPP waste-to-energy projects in China," *Applied Energy*, vol. 158, pp. 403–411, Nov. 2015, doi: 10.1016/j.apenergy.2015.08.043.
- [90] M. S. S. Danish, T. Senjyu, H. Zaheb, N. R. Sabory, A. M. Ibrahim, and H. Matayoshi, "A novel transdisciplinary paradigm for municipal solid waste to energy," *Journal of Cleaner Production*, vol. 233, pp. 880–892, Oct. 2019, doi: 10.1016/j.jclepro.2019.05.402.
- [91] E. de Titto and A. Savino, "Environmental and health risks related to waste incineration," *Waste Manag Res*, vol. 37, no. 10, pp. 976–986, Oct. 2019, doi: 10.1177/0734242X19859700.
- [92] L. Strano, D. V. Pecoraro, N. Pecoraro, C. Gigli, and G. Amara, "Communication as a Prevention Tool: A Key Lever for General Acceptance of the Role of Incineration (Waste-to-Energy) and Transformation plants towards Circular Economy," 2019.
- [93] T. Casti, "Waste to Energy in Denmark: Danish legal pathway to a clean Waste to Energy," Master Thesis, University of Oslo, Faculty of Law, Oslo, Norway, 2020. [Online]. Available: <https://www.duo.uio.no/bitstream/handle/10852/81229/1/Teresa-Casti---Master-Thesis---15-August.pdf>
- [94] W. P. Utama, A. Wibowo, D. Y. Jumas, E. Rita, M. Peli, and Yulcherlina, "Risk allocation of PPP waste to energy projects in Indonesia: A research framework," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 930, no. 1, p. 012023, Sep. 2020, doi: 10.1088/1757-899X/930/1/012023.

- [95] T. Cole-Hunter *et al.*, “The health impacts of waste-to-energy emissions: a systematic review of the literature,” *Environ. Res. Lett.*, vol. 15, no. 12, p. 123006, Dec. 2020, doi: 10.1088/1748-9326/abae9f.
- [96] P. Ghaebi Panah, R.-A. Hooshmand, M. Gholipour, and M. Bornapour, “Urban microgrid ancillary service provision using plugin electric vehicle and waste-to-energy CHP,” *Journal of Energy Storage*, vol. 29, p. 101413, Jun. 2020, doi: 10.1016/j.est.2020.101413.
- [97] P. M. Nordestgaard and C. H. Arndt, “AMAGER BAKKE: A steel building with the design challenge of creating a world famous recreational roof,” *ce/papers*, vol. 3, no. 3–4, pp. 151–156, 2019, doi: 10.1002/cepa.1156.
- [98] V. Bisinella, J. Nedenskov, C. Riber, T. Hulgaard, and T. H. Christensen, “Environmental assessment of amending the Amager Bakke incineration plant in Copenhagen with carbon capture and storage.” Accessed: Feb. 22, 2023. [Online]. Available: <https://journals.sagepub.com/doi/epub/10.1177/0734242X211048125>
- [99] C. B. Agaton, C. S. Guno, R. O. Villanueva, and R. O. Villanueva, “Economic analysis of waste-to-energy investment in the Philippines: A real options approach,” *Applied Energy*, vol. 275, p. 115265, Oct. 2020, doi: 10.1016/j.apenergy.2020.115265.
- [100] N. G. Leveson, M. Daouk, N. Dulac, and K. Marais, “Applying STAMP in Accident Analysis,” Massachusetts Institute of Technology. Engineering Systems Division, Working Paper, Jun. 2003. Accessed: May 05, 2021. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/102905>
- [101] W. Young and N. Leveson, “Systems thinking for safety and security,” in *Proceedings of the 29th Annual Computer Security Applications Conference*, in ACSAC '13. New York, NY, USA: Association for Computing Machinery, Dec. 2013, pp. 1–8. doi: 10.1145/2523649.2530277.
- [102] C. H. Fleming, “Safety-driven early concept analysis and development,” Thesis, Massachusetts Institute of Technology, 2015. Accessed: Mar. 14, 2023. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/97352>
- [103] M. Chaal, O. A. Valdez Banda, J. A. Glomsrud, S. Basnet, S. Hirdaris, and P. Kujala, “A framework to model the STPA hierarchical control structure of an autonomous ship,” *Safety Science*, vol. 132, p. 104939, Dec. 2020, doi: 10.1016/j.ssci.2020.104939.
- [104] S. Sultana, P. Okoh, S. Haugen, and J. E. Vinnem, “Hazard analysis: Application of STPA to ship-to-ship transfer of LNG,” *Journal of Loss Prevention in the Process Industries*, vol. 60, pp. 241–252, Jul. 2019, doi: 10.1016/j.jlp.2019.04.005.
- [105] I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, “STPA-SafeSec: Safety and security analysis for cyber-physical systems,” *Journal of Information Security and Applications*, vol. 34, pp. 183–196, Jun. 2017, doi: 10.1016/j.jisa.2016.05.008.
- [106] A. L. Dakwat and E. Villani, “System safety assessment based on STPA and model checking,” *Safety Science*, vol. 109, pp. 130–143, Nov. 2018, doi: 10.1016/j.ssci.2018.05.009.
- [107] T. Bjerga, T. Aven, and E. Zio, “Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM,” *Reliability Engineering & System Safety*, vol. 156, pp. 203–209, Dec. 2016, doi: 10.1016/j.ress.2016.08.004.
- [108] D. G. C. Jamot and J. Y. Park, “System theory based hazard analysis for construction site safety: A case study from Cameroon,” *Safety Science*, vol. 118, pp. 783–794, Oct. 2019, doi: 10.1016/j.ssci.2019.06.007.
- [109] S. M. Sulaman, A. Beer, M. Felderer, and M. Höst, “Comparison of the FMEA and STPA safety analysis methods—a case study,” *Software Qual J*, vol. 27, no. 1, pp. 349–387, Mar. 2019, doi: 10.1007/s11219-017-9396-0.
- [110] C. Fleming and N. G. Leveson, *Including safety during early development phases of future air traffic management concepts*. 2015.
- [111] International Accreditation Forum, Inc, “International Accreditation Forum - IAF. Find Members, publications & resources.” Accessed: Sep. 07, 2020. [Online]. Available: <https://www.iaf.nu/>
- [112] International Organization for Standardization, “ISO 22000:2018, Food safety management systems - Requirements for any organization in the food chain.” ISO, Geneva, Switzerland, 2018. Accessed: Jul. 14, 2020. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/54/65464.html>

- [113] International Organization for Standardization, “ISO 50001:2018, Energy management systems - Requirements with guidance for use.” ISO, Geneva, Switzerland, 2018. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/94/69426.html>
- [114] International Organization for Standardization, “ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements.” ISO, Geneva, Switzerland, 2019. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/51/75106.html>
- [115] International Organization for Standardization, “ISO/IEC 20000-1:2018, Information technology - Service management - Part 1: Service management system requirements.” ISO, Geneva, Switzerland, 2018. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/06/70636.html>
- [116] International Organization for Standardization, “ISO 28000:2007, Specification for security management systems for the supply chain.” ISO, Geneva, Switzerland, 2007.
- [117] International Organization for Standardization, “ISO 37001:2016, Anti-bribery management systems — Requirements with guidance for use.” ISO, Geneva, Switzerland, 2016. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/50/65034.html>
- [118] International Organization for Standardization, “ISO 39001:2012, Road traffic safety (RTS) management systems - Requirements with guidance for use.” ISO, Geneva, Switzerland, 2012.
- [119] International Organization for Standardization, “ISO Guide 73:2009, Risk management - Vocabulary.” ISO, Geneva, Switzerland, 2009.
- [120] International Organization for Standardization, “ISO/IEC 27005:2018, Information technology - Security techniques - Information security risk management.” ISO, Geneva, Switzerland. Accessed: Jul. 13, 2020. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html>
- [121] International Electrotechnical Commission, “IEC 62366-1:2015, Medical devices - Part 1: Application of usability engineering to medical devices.” IEC, Geneva, Switzerland, 2015.
- [122] “Cambridge Dictionary, turnkey contract.” Accessed: Jun. 23, 2023. [Online]. Available: <https://dictionary.cambridge.org/dictionary/english/turnkey-contract>
- [123] A. A. Adesina, Q. Hussain, S. Pandit, M. Rejzek, and A. M. Hochberg, “Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management,” *Pharm Med*, vol. 31, no. 4, pp. 267–278, Aug. 2017, doi: 10.1007/s40290-017-0195-5.
- [124] T. Pawlicki, A. Samost, D. W. Brown, R. P. Manger, G.-Y. Kim, and N. G. Leveson, “Application of systems and control theory-based hazard analysis to radiation oncology,” *Medical Physics*, vol. 43, no. 3, pp. 1514–1530, 2016, doi: 10.1118/1.4942384.
- [125] B. Antoine, “Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems : an example from the medical device industry,” Thesis, Massachusetts Institute of Technology, 2013. Accessed: Jul. 02, 2021. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/79424>
- [126] N. Silvis-Cividjian, W. Verbakel, and M. Admiraal, “Using a systems-theoretic approach to analyze safety in radiation therapy—first steps and lessons learned,” *Safety Science*, vol. 122, p. 104519, Feb. 2020, doi: 10.1016/j.ssci.2019.104519.
- [127] S. Yamaguchi, “A system safety analysis of tomographic treatment,” Thesis, Massachusetts Institute of Technology, 2017. Accessed: Jul. 04, 2021. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/113531>
- [128] M. Rejzek, “Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System,” p. 22, 2012.
- [129] A. Tang, A. Samost, A. Viswanathan, R. Cormack, and A. Damato, “WE-G-BRA-07: Analyzing the Safety Implications of a Brachytherapy Process Improvement Project Utilizing a Novel System-Theory-Based Hazard-Analysis Technique,” *Medical Physics*, vol. 42, no. 6Part40, pp. 3692–3692, 2015, doi: 10.1118/1.4926077.
- [130] R. Martin and C. Hilbes, *Use of STPA in digital instrumentation and control systems of nuclear power plants*. Gesellschaft für Informatik e.V., 2014. Accessed: Jul. 04, 2021. [Online]. Available: <http://dl.gi.de/handle/20.500.12116/2961>

- [131] S. S. Krauss, M. Rejzek, and C. Hilbes, "Tool Qualification Considerations for Tools Supporting STPA," *Procedia Engineering*, vol. 128, pp. 15–24, Jan. 2015, doi: 10.1016/j.proeng.2015.11.500.
- [132] F. Ackermann, C. Eden, T. Williams, and S. Howick, "Systemic risk assessment: a case study," *Journal of the Operational Research Society*, vol. 58, no. 1, pp. 39–51, Jan. 2007, doi: 10.1057/palgrave.jors.2602105.
- [133] J. Qin, Y. Xi, and W. Pedrycz, "Failure mode and effects analysis (FMEA) for risk assessment based on interval type-2 fuzzy evidential reasoning method," *Applied Soft Computing*, vol. 89, p. 106134, Apr. 2020, doi: 10.1016/j.asoc.2020.106134.
- [134] M. Titko, J. Ristvej, and Z. Zamiar, "Population Preparedness for Disasters and Extreme Weather Events as a Predictor of Building a Resilient Society: The Slovak Republic," *International Journal of Environmental Research and Public Health*, vol. 18, no. 5, Art. no. 5, Jan. 2021, doi: 10.3390/ijerph18052311.
- [135] D. Kahneman and A. Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica*, vol. 47, pp. 263–291, Mar. 1979.
- [136] D. Kahneman and A. Tversky, "Prospect Theory: An Analysis of Decision Under Risk," in *Handbook of the Fundamentals of Financial Decision Making*, vol. Volume 4, in World Scientific Handbook in Financial Economics Series, no. Volume 4, vol. Volume 4. , WORLD SCIENTIFIC, 2012, pp. 99–127. doi: 10.1142/9789814417358_0006.
- [137] D. Kahneman, *Kahneman, D., Thinking, Fast and Slow*. Macmillan, NY, USA, 2011.
- [138] S. C. Ward and C. B. Chapman, "Risk-management perspective on the project lifecycle," *International Journal of Project Management*, vol. 13, no. 3, pp. 145–149, Jun. 1995, doi: 10.1016/0263-7863(95)00008-E.
- [139] P. W. G. Morris, J. Pinto, and J. Söderlund, "Introduction: Towards the Third Wave of Project Management," in *The Oxford Handbook of Project Management*, P. W. G. Morris, J. Pinto, and J. Söderlund, Eds., Oxford University Press, 2011, p. 0. doi: 10.1093/oxfordhb/9780199563142.003.0001.
- [140] H. Thamhain, "Managing Risks in Complex Projects," *Project Management Journal*, vol. 44, no. 2, pp. 20–35, 2013, doi: 10.1002/pmj.21325.
- [141] L. H. Rodrigues-da-Silva and J. A. Crispim, "The Project Risk Management Process, a Preliminary Study," *Procedia Technology*, vol. 16, pp. 943–949, Jan. 2014, doi: 10.1016/j.protcy.2014.10.047.
- [142] P. Cirillo and N. N. Taleb, "Tail risk of contagious diseases," *Nat. Phys.*, vol. 16, no. 6, Art. no. 6, Jun. 2020, doi: 10.1038/s41567-020-0921-x.
- [143] A. Nieto-Morote and F. Ruz-Vila, "A fuzzy approach to construction project risk assessment," *International Journal of Project Management*, vol. 29, no. 2, pp. 220–231, Feb. 2011, doi: 10.1016/j.ijproman.2010.02.002.
- [144] N. Green, "Keys to Success in Managing a Black Swan Event," *AON Corporation*, 2011, [Online]. Available: https://www.aon.com/attachments/risk-services/Manage_Black_Swan_Even_Whitepaper_31811.pdf
- [145] S. H. Björnsdóttir, "Comparison of Risk Analysis Methodologies," MIT STAMP/STPA Workshop, Massachusetts Institute of Technology, Cambridge, Massachusetts, Mar. 2015. Accessed: May 06, 2024. [Online]. Available: <http://psas.scripts.mit.edu/home/wp-content/uploads/2015/04/Bjornsdottir-STAMP-MIT-2015.pdf>
- [146] S. H. Björnsdóttir, "Comparison of Risk Analysis Methodologies in an Electrical Grid," 3rd European STAMP/STPA Workshop, Amsterdam University of Applied Sciences, the Netherlands, Oct. 2015. Accessed: May 06, 2025. [Online]. Available: <https://www.amsterdamuas.com/binaries/content/assets/subsites/aviation/stamp/2015/presentations/day-2/svana-helen-bjornsdottir---comparison-of-risk-analysis-methodologies-in-an-electrical-grid.pdf?1445518523159>
- [147] S. H. Björnsdóttir, "Risk Analysis in Design and Construction of a Hydropower Station," 4th European STAMP/STPA Workshop, Zürich University of Applied Sciences, Zürich, Switzerland, Sep. 2016. Accessed: May 06, 2024. [Online]. Available: <https://slideplayer.com/slide/11765611/>

- [148] C. R. Brown, J. Zheng, S. H. Björnsdóttir, and M. Rejzek, “STPA Software Module,” 5th European STAMP/STPA Workshop and Conference, Reykjavik University, Iceland, Sep. 2017. Accessed: May 06, 2024. [Online]. Available: https://en.ru.is/media/veldu-flokk/ESW2017-Stiki_RMS_STAMP-STPA_2017_CRB.pdf
- [149] S. Björnsdóttir, C. R. Brown, and M. Rejzek, “The Challenges of Supporting STPA with a Software Tool,” Mar. 2018. Accessed: May 06, 2024. [Online]. Available: <https://psas.scripts.mit.edu/home/wp-content/uploads/2018/04/SupportingSTPAwithSoftwareTools.pdf>
- [150] S. H. Björnsdóttir, “The various facets of risk - Proposed WtE project in Iceland,” IMaR conference, Reykjavik University, Iceland, Oct. 20, 2022. Accessed: May 06, 2024. [Online]. Available: <https://static1.squarespace.com/static/625b312b29252c11b0f1c346/t/635bb38d52d90a16d77e52df/1666954127595/Svana+Helen++the+various...pdf>
- [151] S. H. Björnsdóttir, “WtE preliminary project in Iceland - Assessing and dealing with different facets of risk,” Apr. 18, 2024. [Online]. Available: <https://static1.squarespace.com/static/625b312b29252c11b0f1c346/t/66205f9d5bbb5c516fbc3f60/1713397662944/IMaR+2024++SHB+WtE+risk+assessment.pdf>
- [152] K. D. Sigurðardóttir, “Application of system safety to design and construction of a hydropower station,” Thesis, Reykjavik University, 2016. Accessed: May 06, 2024. [Online]. Available: <https://skemman.is/handle/1946/25611>
- [153] K. D. Sigurðardóttir, P. Jansson, S. H. Björnsdóttir, and N. Leveson, “Application of System Safety to Design and Construction of a Hydropower Station,” 4th European STAMP/STPA Workshop, Zürich University of Applied Sciences, Zürich, Switzerland, Sep. 2016. [Online]. Available: https://www.zhaw.ch/storage/engineering/institute-zentren/iamp/sp_sks/ESW2016/Poster-Sigurardottir-ApplicationOfSystemSafetyToDesignAndConstructionHydropowerStation.pdf
- [154] H. Einarsdóttir, “Comparison of the application of risk management to medical devices guided by ISO 14971 and STAMP,” Thesis, Reykjavik University, 2017. Accessed: May 06, 2024. [Online]. Available: <https://skemman.is/handle/1946/28776>
- [155] Þ. Jóhannsson, “Supply chain risk assessment,” Thesis, Reykjavik University, 2015. Accessed: May 06, 2024. [Online]. Available: <https://skemman.is/handle/1946/22333>
- [156] E. Alexandersson, “Risk management and value creation : an international high-tech manufacturing company’s approach to risk management and value creation in new product development projects,” Thesis, Reykjavik University, 2023. Accessed: May 06, 2024. [Online]. Available: <https://skemman.is/handle/1946/44764>
- [157] S. H. Björnsdóttir and M. Rejzek, “Embedding STPA into a Highly Successful Risk Management Software Application,” Mar. 2017. [Online]. Available: <https://digitalcollection.zhaw.ch/bitstream/11475/16831/2/212849.pdf>
- [158] S. H. Björnsdóttir, “STPA Software Solution,” Risk Management Studio. Accessed: May 09, 2024. [Online]. Available: <https://www.riskmanagementstudio.com/stpa-software-solution/>
- [159] M. Rejzek, S. H. Björnsdóttir, and S. S. Krauss, “Modelling Multiple Levels of Abstraction in Hierarchical Control Structures,” Sep. 15, 2017. Accessed: Jul. 02, 2021. [Online]. Available: http://www.ijssca.com/DOI_ISSJ/02012018/2018020194103.html
- [160] W. Young and N. G. Leveson, “An Integrated Approach to Safety and Security Based on Systems Theory,” *Commun. ACM*, vol. 57, no. 2, pp. 31–35, Feb. 2014, doi: 10.1145/2556938.
- [161] “Systems Theory - An Overview.” Accessed: Jul. 05, 2021. [Online]. Available: <https://www.sciencedirect.com/topics/psychology/systems-theory>
- [162] International Organization for Standardization, “ISO Strategy 2016-2020.” Accessed: May 22, 2017. [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_strategy_2016-2020.pdf
- [163] Katie Bird, “Four trends will impact ISO’s future strategy,” ISO. Accessed: Jul. 13, 2020. [Online]. Available: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2019/09/Ref2436.html>

Glossary

A glossary of terms and definitions that appear in this thesis.

Term	Definition	References
Accident	Something bad that happens that is not expected or intended and that often damages something or injures someone.	Cambridge dictionary
Accredited	Officially recognized or approved, officially accepted as being of a particular standard.	Cambridge dictionary
Ambiguity	The fact of something having more than one possible meaning and therefore possibly causing confusion; a situation in which something has more than one possible meaning and may therefore cause confusion.	Cambridge dictionary
Audit	Degree to which a set of inherent characteristics of an object fulfils requirements.	ISO 9000:2015
Benchmarking	The act of measuring the quality of something by comparing it with something else of an accepted standard.	Cambridge dictionary
Black swan	A term popular in risk management, based upon a book of the same name in which the author defines a Black Swan as an event that has not been predicted by normal scientific or probability methods.	The Black Swan: Second Edition: The Impact of the Highly Improbable, by Nassim Nicholas Taleb.
Business continuity	The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level	ISO 22301:2019
Business continuity management	Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.	ISO 22301:2019
Consequence	Outcome of an event affecting objectives.	ISO Guide 73:2009

Term	Definition	References
Control theory	A field of mathematics and engineering dealing with monitoring and controlling the behavior of certain physical processes and systems to produce the desired or best outcome.	American Psychological Association dictionary
Controller	A device used to operate or control a machine, a computer game etc., or a person who controls something, or someone who is responsible for what a particular organization does	
Complex	Involving a lot of different but related parts, having many parts related to each other in ways that may be difficult to understand.	Cambridge dictionary
Diagram	Multiple diagrams can be used to represent one STAMP model.	Article D
EBITDA	Earnings Before Interest, Tax, Depreciation and Amortization: a company's profits in a particular period, before taking away amounts for interest paid, tax paid, and the decrease in the value of things that the company owns.	Cambridge dictionary
Element	Element in a STAMP diagram: controller, controlled process, control action or feedback.	Article D
Establishing the context	Defining the external and internal parameters to be taken into account when managing risk and setting the scope and risk criteria for the risk management policy.	ISO Guide 73:2009
Eurostars	Eurostars is part of the European Partnership on Innovative SMEs. The partnership is co-funded by the European Union through Horizon Europe.	Eureka
Event	Occurrence or change of a particular set of circumstances.	ISO Guide 73:2009
Fat tail event	An event of significant magnitude that takes place or is observed at the end-or tail- of a bell curve- i.e., a normal distribution curve- (hence it is a rare event). It represents a statistical irregularity that falls outside the expected normal distribution. In the financial markets, fat-tail events come in the form of crashes, burst bubbles, panics, and other crises.	The Financial Encyclopedia, FINcyclopedia
Harm	Injury or damage to the health of people, or damage to property or the environment.	ISO 14971:2019
Hazard	Source of potential harm.	ISO Guide 73:2009
Indicator	Measure that provides an estimate or evaluation of specified attributes derived from an analytical	ISO/IEC 27000:2017

Term	Definition	References
	model with respect to defined information needs.	
Incident	An event which is not part of standard business operations which may impact or interrupt services and, in some cases, may lead to disaster. A situation that might be, or could lead to, a disruption, loss, emergency or crisis.	The Business Continuity Institute
Incineration	The process of burning something completely. Incineration is a waste treatment process that involves the combustion of substances contained in waste materials. Industrial plants for waste incineration are commonly referred to as waste-to-energy facilities.	Cambridge dictionary
Information security	Preservation of confidentiality, integrity and availability of information.	ISO/IEC 27000: 2017
Landfill	The process of getting rid of large amounts of rubbish by burying it, or a place where rubbish is buried	Cambridge dictionary
Likelihood	Chance of something happening	ISO Guide 73:2009
Loss	Unrecoverable resources that are redirected or removed as a result of a Business Continuity event. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.	Business Continuity Institute / Disaster Recovery Journal
Management system	Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives.	ISO 22301:2019
Megaproject	Megaprojects are large-scale, complex ventures that typically cost \$1 billion or more, take many years to develop and build, involve multiple public and private stakeholders, are transformational, and impact millions of people	The Oxford Handbook of Megaproject Management
Model	A model of an object (e.g., activity, system) is a simplified representations of this object.	Society for Risk Analysis Glossary
Organization	A person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives.	ISO 22301:2019
Probability	Measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty.	ISO Guide 73:2009
Procedure	A specified way to carry out an activity or a process.	ISO 9000:2015

Term	Definition	References
Process	A set of interrelated or interacting activities that use inputs to deliver an intended result.	ISO 9000:2015
Qualitative	Relating to how good or bad something is	Cambridge dictionary
Quality	Degree to which a set of inherent characteristics of an object fulfils requirements.	ISO 9000:2015
Quantitative	Relating to an amount that can be measured	Cambridge dictionary
Questionnaire	A list of questions that several people are asked so that information can be collected about something.	Cambridge dictionary
Residual risk	Risk remaining after risk treatment.	ISO Guide 73:2009
Resilience	Adaptive capacity of an organization in a complex and changing environment.	ISO Guide 73:2009
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.	ISO Guide 73:2009
Risk	<p>(a) Effect of uncertainty on objects.</p> <p>(b) A future activity [interpreted in a wide sense to also cover, for example, natural phenomena], for example the operation of a system, and define risk in relation to the consequences (effects, implications) of this activity with respect to something that humans value. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is often on negative, undesirable consequences. There is always at least one outcome that is considered as negative or undesirable. Overall qualitative definitions:</p> <ol style="list-style-type: none"> 1. Risk is the possibility of an unfortunate occurrence 2. Risk is the potential for realization of unwanted, negative consequences of an event 3. Risk is exposure to a proposition (e.g., the occurrence of a loss) of which one is uncertain 4. Risk is the consequences of the activity and associated uncertainties 5. Risk is uncertainty about and severity of the consequences of an activity with respect to something that humans value 6. Risk is the occurrences of some specified consequences of the activity and associated uncertainties 7. Risk is the deviation from a reference value 	<p>ISO Guide 73:2009</p> <p>Society for Risk Analysis</p>

Term	Definition	References
	and associated uncertainties	
Risk analysis	Systematic process to comprehend the nature of risk and to express the risk, with the available knowledge. Risk analysis is often also understood in a broader way, in particular in the Society for Risk Analysis (SRA) community: risk analysis is defined to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level.	Society for Risk Analysis
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.	ISO Guide 73:2009
	Systematic process to comprehend the nature of risk, express and evaluate risk, with the available knowledge.	Society of Risk Analysis
Risk control	Measure that is modifying risk.	ISO Guide 73:2009
Risk criteria	Terms of references against which the significance of a risk is evaluated.	ISO Guide 73:2009
Risk event	Risk Event denotes the concrete realization (manifestation) of an abstract Risk. It offers ex-post (materialized) evidence for what was earlier only a potentiality (Event Risk). Depending on the nature (for example severity) of the risk event, alternative terms used might be Incident or Disaster. While in principle all risk realizations are "events", the term is informally used to denote realizations that manifest within a narrow interval of time (where narrowness is defined with respect e.g., to the Risk Horizon).	Open Risk Manual
Risk factor	Something that increases risk or susceptibility.	Merriam-Webster dictionary
Risk identification	Process of finding, recognizing and describing risks.	ISO Guide 73:2009
Risk management	Coordinated activities to direct and control an organization with regard to risk.	ISO Guide 73:2009
Risk management framework	Set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and	ISO Guide 73:2009

Term	Definition	References
	continually improving risk management throughout the organization.	
Risk management process	Systematic application of management policies, procedures and practices to the activities of communication, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk.	ISO Guide 73:2009
Risk mitigation	Process of actions to reduce risk.	Society for Risk Analysis
	Implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner. Activities taken to reduce the severity or consequences of an emergency	Business Continuity Institute
Risk source	Element which alone or in combination has the potential to give rise to risk.	ISO Guide 73:2009
Risk treatment	Process of actions to modify risk.	Society for Risk Analysis
Safety	A state in which or a place where you are safe and not in danger or at risk	Cambridge dictionary
Scenario	One of several possible situations that could exist in the future.	Cambridge dictionary
Secure	Without unacceptable risk when restricting the concept of risk to intentional acts by intelligent actors.	Society for Risk Analysis
Security	Interpreted in the same way as secure (for example when saying that security is achieved). The antonym of risk when restricting the concept of risk to intentional acts by intelligent actors (the security level is linked to the risk level; a high security level means a low risk and vice versa).	Society for Risk Analysis
Stakeholder	An employee, investor, customer, etc. who is involved in or buys from a business and has an interest in its success.	Cambridge dictionary
System	Set of interrelated or interacting elements.	ISO 9000:2015
System risk	Potential difficulties, such as failure of one participant or part of a process, system, industry or market to meet its obligations, that could cause other participants to not meet their	Business Continuity Institute

Term	Definition	References
	obligations; this could cause liquidity and other problems, thereby threatening stability of the whole process, system, industry or market.	
Systemic risk	The risk that the failure of one financial institution (such as a bank) could cause other interconnected institutions to fail and harm the economy as a whole.	Merriam-Webster dictionary
Systems theory	Systems theory is a theory of interacting processes and the way they influence each other over time to permit the continuity of some larger whole.	Encyclopedia of Human Behavior (Second Edition), 2012
Stakeholder	Person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity.	ISO Guide 73:2009
Uncertain	Unclear, or not sure.	Cambridge dictionary
Volatile	Likely to change often or suddenly and unexpectedly	Cambridge dictionary
Vulnerability	Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with consequence.	ISO Guide 73:2009

Acronyms

List of acronyms that appear in this thesis.

AS/NZS	Australian and New Zealand standards
BCI	Business Continuity Institute
BSI	British Standards Institute
CA	Control Action
CAPEX	Capital Expenditure
ConOps	Concept of Operations
CS	Control Structure
EBITDA	Earnings Before Interest, Tax, Depreciation and Amortization
EEA	European Economic Area
EERMF	Enhanced Enterprise Risk Management Framework
ESG	Environmental, Social and Governance
EU	European Union
FMEA	Failure Mode and Effects Analysis
FRAM	Functional Resonance Analysis Method
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability
HCS	Hierarchical Control Structure
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MSS	Management System Standard
MSW	Municipal Solid Waste
NIST	National Institute of Standards and Technology (USA)
OPEX	Operational Expenditure
PMI	Project Management Institute
PPP	Public-Private Partnership
PRA	Probabilistic Risk Analysis
RA	Risk Analysis
STAMP	Systems-Theoretic Accident Model and Processes

STECA	Systems-Theoretic Early Concept Analysis
STPA	Systems-Theoretic Process Analysis
STPA-Sec	Systems-Theoretic Process Analysis for Security
SLC	System-Level Constraint
SLH	System-Level Hazard
SLL	System-Level Loss
SRA	The Society for Risk Analysis
UPPAAL	Uppsala University (UPP) in Sweden and Aalborg University (AAL) in Denmark
UCA	Unsafe Control Action
VUCA	Volatility, Uncertainty, Complexity and Ambiguity
WMA	Waste Municipal Association
WtE	Waste-to-Energy

Appendices

Article A

The Importance of Risk Management: What is Missing in ISO Standards?

The Importance of Risk Management: What is Missing in ISO Standards?

Svana Helen Björnsdóttir,^{1,*} Páll Jenson,¹ Robert J. de Boer,²
and Saemundur E. Thorsteinsson³

The overall aim of this article is to contribute to the further development of the area of risk analysis and risk management in the International Organization for Standardization (ISO) standards by strengthening its scientific basis. Industrial standards, especially ISO standards, are the tools organizations use to manage their risk, through following their guidance and complying with their requirements. Organizations confirm their compliance with these standards through certification, which means that they heavily depend upon the quality of the ISO standards to enable them to effectively manage their risk. The purpose of this study is to investigate what guidance is given on key elements of risk management and how well ISO standards are aligned with state-of-the-art risk management literature. Eighteen ISO standards, all addressing risk management, were reviewed in this study with regard to risk terminology and guidance. The results of the study confirm the increasing importance of risk management for business. However, the study also shows a lack of guidance on doing risk analysis in the industrial standards examined. The ISO management system standards and guidelines are not aligned with the scientific literature on risk and are not appropriate for the management of risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems.

KEY WORDS: ISO standards; risk analysis; risk management

1. INTRODUCTION

Risk management is increasingly important for business. It has even become mandatory in data protection in Europe (Parliament and Council of the European Union, 2016). According to the Global Risks Report 2020 and 2021, published by the World Economic Forum, the global economy is facing increased risks in many areas and therefore the societal need for protection from harm is also increas-

ing (The Global Risks Report 2020, 2020; The Global Risks Report 2021, 2021). This results in governmental pressure on organizations to demonstrate that they are managing risk appropriately. Standardization of risk management through compliance with industrial standards allows organizations to demonstrate their efforts in this area. This article discusses the most widespread International Organization for Standardization (ISO) standards, the management system standards (MSSs) included in the annual ISO survey 2019 (International Organization for Standardization, 2020), and the guidelines they refer to, and what they say about risk management.

The rest of this section discusses the motivation and aim of this study, and development of ISO standards and their increasing focus on risk management. Section 2 discusses important recent developments

¹Department of Engineering, Reykjavik University, Reykjavik, Iceland.

²SDO University of Applied Sciences, Maassluis, The Netherlands.

³University of Iceland, Reykjavik, Iceland.

*Address correspondence to Svana Helen Björnsdóttir, Department of Engineering, Reykjavik University, Menntavegur 1, IS-102 Reykjavik, Iceland; svanahb@ru.is.

within the scientific field of risk based on review of literature and presents state-of-the-art thinking on risk. Section 3 describes the research methodology. It describes the selection of ISO standards, and the execution of the search for description of risk analysis in the standards. Section 4 presents the results of this study. Section 5 summarizes the results and recommends improvements. Section 6 contains conclusions and thoughts on future work.

1.1. Motivation and Aim of the Study

Risk management is more than compliance with requirements of standards. According to both ISO Guide 73 (International Organization for Standardization, 2009) and ISO 31000 (International Organization for Standardization, 2018b), risk is defined as “effect of uncertainties on objectives” and risk management is defined as “coordinated activities to direct and control an organization with regard to risk.” ISO 31000 furthermore defines risk management as a process that comprises six main activities: (1) communicating and consulting; (2) establishing the context; (3) assessing risk; (4) treating risk; (5) monitoring and reviewing; and (6) recording and reporting. Risk assessment is further divided into risk identification, risk analysis, and risk evaluation. Risk analysis involves developing an understanding of the risk, considering the causes and sources of risk, describing positive and negative consequences, and assessing the likelihood that those consequences can occur. Risk analysis is therefore a critical part of risk management if risk is to be treated in a manageable and appropriate manner. ISO 31000 recommends that organizations integrate the process for managing risk into their overall governance, strategy, and processes in a systematic, transparent, and credible manner.

In recent years, technology has increasingly merged with the management and organizations activities, for example, in the form of a variety of smart solutions and automation. At the same time, risk management has become an important part of business management and decision making. This trend can be seen from the number of ISO certifications in ISO surveys shown in Table I for the years 2014–2019. All MSSs in the ISO survey 2019 address risk management in one way or another.

Fast evolving technology and ever greater complexity in sociotechnical systems challenge risk management today to capture risk that arises from interactions between people and systems, taking into account emergent behavior and nonlinear causal

relations. Standards are widely used in industry, and they have a major impact on regulations in societies. Their use is voluntary, but in many areas, such as safety and security, ISO standards have become the norm in legislation and official supervision (Aven & Ylönen, 2019; International Organization for Standardization, 2016a). It is important that usage of and compliance with standards prove to be useful in challenging real-case risk management and do not give people a false sense of safety and security.

Many organizations depend heavily on information and/or technology for their principal business. They face the challenge of how to keep their infrastructure up to date without either jeopardizing their ability to function or breaking the budget. Their managers expect international standards to provide guidance to help them tailor their risk management system to their organizations. It is uncertain whether current risk management standards provide sufficient guidance and are suitable as tools for identifying risk scenarios that encompass the entire risk process in increasingly complex systems (Carayon *et al.*, 2015; Carreras, Newman, Dobson, Lynch, & Gradney, 2014; Dekker, Cilliers, & Hofmeyr, 2011; Holovatch, Kenna, & Thurner, 2017; Leveson, 2004), and whether traditional standards approach is appropriate to effectively manage risk in our complex sociotechnical systems. If not, the original aim to protect society from error, harm, or losses is not being achieved.

The authors' motivation for this study origins in decades of experience working in ISO-certified organizations, as external and internal auditors for information security management systems, management consultants and directors in certified companies. This experience has revealed the importance of ISO standards, not only for businesses but also for societies, the effort in complying with them, and the fact that accredited certification activities are not a guarantee of good risk management. Over the years, certified management systems generally mature and the knowledge and experience that builds up enforces the process of improvement. When unforeseen incidents happen questions arise: Why was this risk not identified? Are there better ways to identify risks and their causal relationship? Could we have designed our systems better with regard to later managing unforeseen risk? Therefore, the aim of this study was twofold: (1) to investigate and evaluate guidance given in ISO standards on risk management, especially for the critical step of risk analysis; and (2) to investigate how well-aligned the standards are with

Table 1. Number of ISO Certifications According to ISO Surveys 2014–2019

ISO Management System Standards	Title	Number of Certifications						
		2019	2018	2017	2016	2015	2014	
ISO 9001:2015 ^{ab}	Quality management systems—Requirements	883,521	878,664	1,058,504	1,105,937	1,034,180	1,036,321	
ISO 14001:2015 ^{ab}	Environmental management systems—Requirements with guidance for use	312,580	307,059	362,610	346,147	319,496	296,736	
ISO 45001:2018 ^{ab}	Occupational health and safety management systems—Requirements with guidance for use	38,654	11,952					
ISO/IEC 27001:2013 ^{ab}	Information technology—Security techniques—Information security management systems—Requirements	36,362	31,910	39,501	33,290	27,536	23,005	
ISO 22000:2005 and 2018 ^a	Food safety management systems—Requirements for any organization in the food chain	33,502	32,120	32,722	32,139	32,061	27,690	
ISO 13485:2003 and 2016 ^a	Medical devices—Quality management systems—Requirements for regulatory purposes	23,045	19,472	31,520	29,585	26,255	26,280	
ISO 50001:2011 and 2018 ^a	Energy management systems—Requirements with guidance for use	18,227	18,059	21,501	20,216	11,985	6,765	

(Continued)

Table I. (Continued)

ISO Management System Standards	Title	Number of Certifications						
		2019	2018	2017	2016	2015	2014	
ISO/IEC 20000-1:2011 and 2018 ^{ab}	Information technology—Service management—Part 1: Service management system requirements	6,047	5,308	5,005	4,537	2,778		
ISO 28000:2007 ^a	Specification for security management systems for the supply chain	1,874	617	494	356			
ISO 22301:2019 ^{ab}	Societal security—Business continuity management systems—Requirements	1,693	1,506	4,281	3,853	3,133	1,757	
ISO 37001:2016 ^{ab}	Anti-bribery management systems	872	389					
ISO 39001:2012 ^{ab}	Road traffic safety (RTS) management systems—Requirements with guidance for use	864	547	620	478			
ISO/TS 16949:2009*—NOT included in ISO survey since 2016	Quality management systems—Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations				67,358	62,944	57,950	
Total number of certifications:		1,357,241	1,307,603	1,556,758	1,576,538	1,457,424	1,418,554	
Change year over year:		3.8%	-16.0%	-1.3%	8.2%	2.7%		

^aRefers to risk management.^bRefers to ISO 31000.

the scientific literature and state-of-the-art thinking on risk. To provide insight on these issues, this article reviews a set of ISO guidelines and compares it with subjects in recent papers on risk science to see if and how ISO guidelines address the main challenges in today's field of risk management. A follow-up study will identify the practical effect of possible caveats.

1.2. Development of ISO Standards and Their Focus on Risk Management

Standards are important because they provide people and organizations with a level of quality, rigor, or specification that is an essential basis for the adequacy of a product or service. They are used as tools to facilitate measurement, manufacturing, commerce, and communication. The ISO is an international standard-setting organization consisting of national standards bodies. ISO defines a standard as a “document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context” (COPOLCO, 2021). As the annual ISO survey shows, there is considerable use of standards in industry and public sectors today. Although ISO standards are meant to be voluntary in use, they have become increasingly important as a benchmark due to their spread and certification schemes. They are even becoming the norm in legislation and by supervisory and regulatory authorities (Aven & Ylönen, 2019; International Organization for Standardization, 2016a; International Organization for Standardization, 2019a). The focus, and some would also say importance, of risk management in business is demonstrated by the number of organizations certified under standards addressing risk.

There are basically two types of ISO standards, the MSSs and the guidelines. An MSS is a standard establishing a set of interrelated or interacting elements of an organization to establish policies and objectives and to develop processes to achieve those objectives. The MSSs are again split into type A and type B (ISO—Management System Standards List, n.d.). Only type A standards contain requirements against which an organization can claim conformance through certification. Note that ISO only develops the standards and is not involved in certification against the standards. Certification bodies not affiliated to ISO perform this function. They can be accredited, but accreditation is not compulsory, and

non-accreditation does not necessarily mean the certification body is not reputable (ISO—Certification, n.d.; International Accreditation Forum, Inc., 2020). However, accreditation does provide independent confirmation of competence.

The annual ISO surveys in Table I shows the growth of certifications globally (International Organization for Standardization, 2020). ISO considers it only feasible to include the most used standards in the survey. Certification bodies are requested to fill out a questionnaire on the number of certificates per country and industry sectors, by standards. The survey counts the number of certificates issued by certification bodies that members of the International Accreditation Forum (IAF) have accredited (International Accreditation Forum, Inc., 2020). The number of standards has increased in past years, and ISO survey 2019 (published in September 2020) included 12 ISO/IEC¹ MSSs (International Organization for Standardization, 2020). Eight of 12 refer to six different ISO/IEC risk management guidelines. These 18 MSSs and guidelines, hereafter referred to as “ISO standards,” create the data source for this study (see Table II).

The 18 ISO standards reviewed in this study are listed with full names below:

- (1) ISO 9001:2015, Quality management systems—Requirements (International Organization for Standardization, 2015a). This is one of the first standards ISO published. Risk was included as an explicit concept in the standard for the first time in 2015. The standard states that it “specifies requirements for the organization to understand its context and determine risk as a basis for planning. This represents the application of risk-based thinking to planning and implementing quality management system processes and will assist in determining the extent of documented information.”
- (2) ISO 14001:2015, Environmental management systems—Requirements with guidance for use (International Organization for Standardization, 2015b). This standard also adopted the risk concept in 2015, like ISO 9001.

¹IEC stands for the International Electrotechnical Commission, an international standards organization that publishes international standards for all electrical, electronic, and related technologies—collectively known as “electrotechnology.”

Table II. List of ISO Standards Reviewed in This Study

Type of Standard ^a	Name of Standard	Purpose of Standard
MSS	ISO 9001	Quality management
MSS	ISO 14001	Environmental management
MSS	ISO 45001	Occupational health and safety
MSS	ISO/IEC 27001	Information security
MSS	ISO 22000	Food safety
MSS	ISO 13485	Medical devices (for regulatory purposes)
MSS	ISO 50001	Energy management
MSS	ISO/IEC 20000-1	Information technology service
MSS	ISO 28000	Supply chain security
MSS	ISO 22301	Societal security and business continuity
MSS	ISO 37001	Anti-bribery security
MSS	ISO 39001	Road traffic safety
Guidelines	ISO 31000	Risk management (general)
Guidelines	IEC 31010	Risk management (risk assessment)
Guidelines	ISO Guide 73	Risk management (vocabulary)
Guidelines	ISO/IEC 27005	Risk management (information security)
Guidelines	ISO 14971	Risk management (medical devices)
Guidelines	IEC 62366-1	Risk management (usability engineering and medical devices)

^aThese standards are examined with regard to consistency in risk terms, guidance (description), and scientific foundation; MSS = Management System Standard.

- (3) ISO/IEC 27001:2013, Information technology—Security techniques—Information security management systems—Requirements (International Organization for Standardization, 2013).
- (4) ISO 22000:2018, Food safety management systems—Requirements for any organization in the food chain (International Organization for Standardization, 2018a).
- (5) ISO 45001:2018, Occupational health and safety management systems—Requirements with guidance for use (International Organization for Standardization, 2018c).
- (6) ISO 13485:2016, Medical devices—Quality management systems—Requirements for regulatory purposes (International Organization for Standardization, 2016a).
- (7) ISO 50001:2018, Energy management systems—Requirements with guidance for use (International Organization for Standardization, 2018d).
- (8) ISO 22301: 2019, Societal security—Business continuity management systems—Requirements (International Organization for Standardization, 2019b).
- (9) ISO/IEC 20000-1:2018, Information technology—Service management—Part 1: Service management system requirements (International Organization for Standardization, 2018e).
- (10) ISO 28000:2007, Specification for security management systems for the supply chain (International Organization for Standardization, 2007).
- (11) ISO 37001:2016, Anti-bribery management systems (International Organization for Standardization, 2016b).
- (12) ISO 39001:2012, Road traffic safety (RTS) management systems—Requirements with guidance for use (International Organization for Standardization, 2012).
- (13) ISO 31000:2018 and 2009, Risk management—Principles and guidelines (International Organization for Standardization, 2018b). First published in 2009, updated 2018. General principles and guidelines on risk management and describes a generic approach for managing any form of risk in a systematic, transparent, and credible manner. To be applied within any scope and context. The only bibliographic reference in ISO 31000 is IEC 31010.
- (14) IEC 31010:2019 and 2009, Risk management—Risk assessment techniques (The International Electrotechnical Commission, 2019). First published in 2009, updated 2019. A dual logo IEC/ISO standard for supporting ISO 31000. It provides guidance on selection and application of systematic techniques for risk assessment. Some

changes have been made regarding bibliographic references in the latest version of IEC 31010:2019. In version 2009, only 11 bibliographic references were made, all to other ISO/IEC standards. In the 2019 version, the bibliographic references are 91. Many of them are not standards but handbooks and they are categorized in the bibliography according to risk techniques with no direct reference to risk science.

- (15) ISO Guide 73:2009 (International Organization for Standardization, 2009) provides a basic risk management vocabulary, for common understanding on risk management concepts and terms in other ISO standards and across different applications. The introduction to the guide states that its aim is “to provide basic vocabulary to develop common understanding on risk management concepts and terms among organizations and functions, and across different applications and types.” Its aim is furthermore to “to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of risk.”
- (16) ISO/IEC 27005:2018 (International Organization for Standardization, n.d.) provides guidelines for information security risk management. The standard supports the general concepts specified in the ISO/IEC 27001 standard and is designed to assist in satisfactory implementation of information security, based on a risk management approach.
- (17) ISO 14971:2019 (International Organization for Standardization, 2019a) is for applying risk management in manufacturing of medical devices. The standard specifies a process for manufacturers to identify the hazards associated with medical devices, to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls. The requirements are meant to apply to all life-cycle stages of a medical device.
- (18) IEC 62366-1:2015 (International Electrotechnical Commission, 2015) is developed jointly by IEC and ISO and provides guidelines for usability engineering to medical device. It specifies a process for manufacturers to analyze, specify, develop, and evaluate the usability

of medical devices as related to safety. It refers to the human factors engineering process that permits the manufacturer to assess and mitigate risks associated with normal use, that is, correct use and use errors. It can be used to identify risks but does not cover abnormal usage.

2. IMPORTANT RECENT DEVELOPMENTS WITHIN THE SCIENTIFIC FIELD OF RISK

This section discusses recent developments and issues within the risk science that are important for the state-of-the-art risk management. It is a literature review with twofold aim. First, to learn what is vital for the state-of-the-art risk management. Second, to review recent literature on ISO standards themselves.

2.1. State-of-the-Art Risk Management

Applying ISO standards is a strategic investment decision. Organizations depend heavily on the guidance given in the standards to effectively manage their risk. Risk management may involve treatment of intangible aspects of assets, values, and services for which guidance or risk assessment criteria can hardly be given in standards for risk management. The user of risk management standards must be aware of this when applying those standards. For the standards to achieve their objective, it is, however, important that the standards address important risk issues and that they are in line with state-of-the-art risk management. In this section, some examples of risk science contributions will be reviewed.

First example is a paper on current trends toward more and wider use of standards by Aven and Ylönén (2019). They emphasize that measures need to be taken to create broader and more scientifically based arenas for guiding risk and safety analysis and management practices. One of these arenas is the Society for Risk Analysis (www.sra.org), established in 1979 in recognition of risk analysis as an emerging discipline (The Society for Risk Analysis [SRA], n.d.). Thompson, Deisler, & Schwing (2005) have documented the motivation and reasons for establishing SRA with primary interests in the impact of risks on human health. Modern-day risk analysis remains a relatively young field and SRA has met a growing need for risk researchers and practitioners to publish their work in a dedicated professional journal,

*Risk Analysis*². It provides a focal point for new developments in the theory and practice of risk analysis in a wide range of disciplines. Some of the literature referred to in this article has been awarded by SRA as the “best paper” on risk analysis, so it seems reasonable to consider that the results presented in them is vital for state-of-the-art risk management. In addition, SRA has defined all major risk terms and claims that their risk glossary (Society for Risk Analysis Glossary, 2018) is unique in its approach compared to existing risk analysis related glossaries, including ISO guidelines, with its incorporation of different perspectives and its systematic separation between overall qualitative concepts and their measurements.

The SRA glossary is founded on the idea that “it is still possible to establish authoritative definitions, the key being to allow for different perspectives on fundamental concepts and to make a distinction between overall qualitative definitions and their associated measurements” (Aven, 2016). The glossary distinguishes between the concept of risk and how it is described or measured, and allows for several definitions, including “risk is the deviation from a reference value and associated uncertainties.” The risk concept allows for both positive and negative consequences (outcomes), but at least one is negative or undesirable. The term risk analysis is used in a narrow sense as a “a systematic process to comprehend the nature of risk and to express the risk, with the available knowledge” and in a broad sense as in the title of this journal to include risk assessment, risk characterization, risk communication, risk management, and policy relating to risk, in the context of risks of concern to individuals, to public and private sector organizations, and to society at a local, regional, national, or global level.

Overall, qualitative definitions of risk are given in SRA’s glossary (Aven, 2016; Society for Risk Analysis Glossary, 2018):

- (1) Risk is the possibility of an unfortunate occurrence.
- (2) Risk is the potential for realization of unwanted, negative consequences of an event.
- (3) Risk is exposure to a proposition (e.g., the occurrence of a loss) of which one is uncertain.
- (4) Risk is the consequences of the activity and associated uncertainties.

- (5) Risk is uncertainty about and severity of the consequences of an activity with respect to something that humans value.
- (6) Risk is the occurrences of some specified consequences of the activity and associated uncertainties.
- (7) Risk is the deviation from a reference value and associated uncertainties.

Examples of risk descriptions/metrics are also given in SRA’s glossary (Aven, 2016; Society for Risk Analysis Glossary, 2018):

- (1) The combination of probability and magnitude/severity of consequences.
- (2) The combination of the probability of a hazard occurring and a vulnerability metric given the occurrence of the hazard.
- (3) The triplet (s_i, p_i, c_i) , where s_i is the i th scenario, p_i is the probability of that scenario, and c_i is the consequence of the i th scenario, $i = 1, 2, \dots, N$.
- (4) The triplet (C', Q, K) , where C' is some specified consequences, Q a measure of uncertainty associated with C' (typically probability), and K the background knowledge that supports C' and Q (which includes a judgment of the strength of this knowledge).
- (5) Expected consequences (damage, loss), further exemplified in the SRA glossary.
- (6) A possibility distribution for the damage (e.g., a triangular possibility distribution).

When comparing risk terminology in ISO standards in Tables III and IV, a comparison with SRA risk terminology is also made in the last columns. The following five papers are examples of risk science contributions that have been rewarded as “best paper” by SRA (Alderson, Brown, & Carlyle, 2015; Aven, 2019; Montibeller & Winterfeldt, 2015; Oughton *et al.*, 2019; Rozell, 2018).

The first paper is from Aven (2019). He questions to which extent the call for a shift from risk to resilience will have implications for the risk field and science. He states that resilience analysis and management is today an integrated part of the risk field and science. Risk analysis in a broad sense is needed to increase relevant knowledge, develop adequate policies, and make the right decisions. Different concerns must be balanced, and limited resources used in an effective way. According to Aven, the resilience arose as a supplement to the traditional probabilistic risk assessment approach. Such approach has

²<https://onlinelibrary.wiley.com/journal/15396924>

Table III. Risk Terminology in ISO Standards

No.	Risk Terminology in ISO Standards/Definition and Description of Risk	ISO 14001: 2015	ISO 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	IEC 31010: 2019	ISO Guide 73: 2009	ISO/IEC 14971: 2019	ISO IEC 62366-1: 2015	Occurrence, Total	SRA Risk Terminology
1	Risk can/must be managed/controlled/ addressed	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	14	
2	Risk is the effect of uncertainty (on objectives)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	11	(Def-5)
3	Risk can be identified/determined	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	11	
4	Risk can be assessed/evaluated	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	11	
5	Risk is characterized by reference to potential events and consequences, or a combination of these																	8	(Def-4)
6	Risk can be analyzed		x															7	
7	Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence			x														7	(Def-4)
8	Risk is associated with threats and/or hazards																	6	

(Continued)

Table III. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk	2013										2018					2015						
		ISO 9001: 2015	ISO 14001: 2015	ISO/IEC 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	IEC 31010: 2019	ISO Guide 73: 2009	ISO/IEC 27005: 2018	ISO 14971: 2019	IEC 62366-1: 2015	Occurrence, Total	SRA Risk Terminology		
9	Risk can change	x	x									x	x	x							5		
10	Risk can be treated/modified			x								x	x	x								5	
11	Risk can provide an opportunity	x	x									x	x	x								5	
12	Risk has different levels/magnitude				x							x	x	x								5	
13	Risk is associated with circumstances											x	x	x								4	
14	Risk is a usability problem (associated with use of software/medical device)																					4	
15	Application of the risk should be related to the objectives of the organization																					4	
16	Changes can result in risks																					4	
17	Risks should be assessed using appropriate methods																					4	
18	Risk can be described																					3	
19	Risk is associated with value of object																					3	(Def-5)
20	Perceptions of risk can vary due to differences in assumptions, concepts, and the needs																					3	

(Continued)

Table III. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk	ISO 9001: 2015	ISO 14001: 2015	ISO/IEC 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	IEC 31010: 2019	ISO Guide 73: 2009	ISO/IEC 14971: 2019	IEC 62366-1: 2015	Occurrence, Total Terminology	SRA Risk
21	Risk is the effect of uncertainty and any such uncertainty can have positive or negative effect												x	x	x				3	(Def-4)
22	Risk is "owned" by someone responsible			x										x	x				3	
23	Risk is combination of the probability of occurrence of harm and the severity (consequences) of that harm						x										x	x	3	Des-1
24	Risk perception is depending upon cultural factors/background												x	x	x				3	
25	Risk can be estimated quantitatively if suitable data are available												x	x	x				3	
26	Risk can arise from contractors'/organization's activities												x	x					3	
27	Risk includes the effects of any of the forms of uncertainty [...] on objectives												x	x	x				3	(Des-4)
28	Risk is associated with vulnerability of object																		3	(Des-2)
29	Risk that is emerging must be identified and treated																		2	

(Continued)

Table III. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk	ISO 9001: 2015	ISO 14001: 2015	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	IEC 31010: 2019	ISO Guide 73: 2009	ISO/IEC 27005: 2018	ISO 14971: 2019	IEC 62366-1: 2015	Occurrence, Total	SRA Risk Terminology
30	Risk can be associated with any activity, process, function, or product												x	x					2	
31	Lack of efficiency can contribute to risk											x						x	2	
32	Risk is triggered by a hazardous state of object (safety risk)																		1	(Des-5)
33	Risk can be introduced by using mobile devices		x																1	
34	Risk can be caused by unauthorized access or changes to the operational environment		x																1	
35	Risk is the relationship of hazard, sequence of events, hazardous situation, and harm																x		1	(Des-2)
36	Risk is related to safety or performance requirements of medical devices or meeting applicable regulatory requirements																	x	1	

(Continued)

Table III. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk	ISO 9001: 2015	ISO 14001: 2015	ISO 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	ISO 31010: 2019	IEC Guide 73: 2009	ISO/IEC 14971: 2019	ISO/IEC 27005: 2018	IEC 62366-1: 2015	Occurrence, Total Terminology	SRA Risk	
37	Risk is associated with the work for which the training or other action is being provided						x														1	
38	There is risk associated with the purchased product and compliance with applicable regulatory requirements						x															1
39	A risk source can be tangible or intangible																					1
40	Risk may be registered in a risk register																					1
41	Occupational health and safety risk is the combination of the likelihood of occurrence of a work-related hazardous event(s) or exposure(s) and the severity of injury and ill health that can be caused by the event(s) and exposure(s)																					1
																						Des-1

(Continued)

Table III. (Continued)

No.	Risk Standards/Definition and Description of Risk	ISO 9001: 2015	ISO 14001: 2015	ISO/IEC 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	IEC Guide 73: 2009	ISO/IEC 14971: 2019	ISO/IEC 27005: 2018	IEC 62366-1: 2015	Occurrence, Total	SRA Terminology	
42	Food safety risk is a function of the probability of an adverse health effect and the severity of that effect, consequential to (a) hazard(s) in food																			1 Des-1	
43	Risk is associated with correct use and use errors, both normal use and abnormal use																				x 1
44	Risk cannot always be tabulated easily as a set of events, their consequences, and their likelihoods																				x 1
	Total number of risk definitions/descriptions per standard:	5	7	11	3	9	6	1	4	6	3	5	24	28	32	3	6	7	7	167	

Note: “x”: appears in the relevant ISO standard; “-”: does not appear in the relevant ISO standard. “Def-N”: in accordance with risk definition no. N in SRA glossary; “(Def-N)”: somewhat in line with SRA glossary. “Des-N”: in accordance with risk description no. N in SRA glossary; “(Des-N)”: somewhat in line with SRA glossary.

Table IV. Description of Risk Analysis in ISO Standards

No.	Risk Terminology in ISO Standards/Definition and Description of Risk Analysis (RA)	ISO 9001: 2015	ISO 14001: 2015	IEC 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 22000: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000- 22301: 2012	ISO 28000: 39001: 2007	ISO 31010: 2018	ISO 37001: 2016	ISO 31000: 2018	IEC 62366- 1: 2015	ISO 14971: 2019	IEC 73: 2005	ISO 2018	IEC 62366- 1: 2015	Occurrence, Definition of RA	SRA
1	RA includes the examination of different sequences of events															x				1	(Def-N)
2	RA is a part of risk assessment															x				1	
3	RA is a systematic use of available information to identify hazards and to estimate the risk															x				1	Def-N
4	Scope of the RA can be very broad or it can be limited																			1	
5	Manufacturer of a medical device shall document the intended use and reasonably foreseeable misuse															x				1	
6	The manufacturer of a medical device shall identify and document those qualitative and quantitative characters that could affect the safety of the medical device																			1	
7	For each identified hazardous situation, the manufacturer shall estimate the associated risk(s) using available information or data—for hazardous situations for which the probability of the occurrence of harm cannot be estimated, the possible consequences shall be listed for use in risk evaluation and risk control																			1	(Def-N)

(Continued)

Table IV. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk Analysis (RA)	ISO 9001: 2015	ISO 14001: 2015	ISO 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 50001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 39001: 2012	ISO 37001: 2016	ISO 31000: 2018	ISO 31010: 2019	ISO Guide 73: 2009	ISO 27005: 2018	ISO 14971: 2019	IEC 62366-1: 2015	Occurrence, Definition of RA	SRRA	
8	RA is a process to comprehend the nature of risk and to determine the level of risk																	x			1	Def-N	
9	RA provides the basis for risk evaluation and decision about risk treatment																	x			1	(Def-N)	
10	RA includes risk estimation																x				2	(Def-N)	
11	Risk management is a systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk								x												1		
12	The organization shall plan actions to address risks and opportunities		x																			1	
13	Actions taken to address risks and opportunities shall be proportionate to the potential impact on the conformity of products and services		x																			1	
14	The risks and opportunities related to environmental aspects can be determined as part of the significance evaluation or determined separately			x																		1	
15	Analyzing security risks includes: (1) assess the potential consequence that would result if the risks identified were to materialize; (2) assess the realistic likelihood of the occurrence of the risks identified; and determine the levels of risk			x																		1	(Def-N)

(Continued)

Table IV. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk Analysis (RA)	ISO 9001: 2015	ISO 14001: 2015	ISO 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 50001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000-1: 2018	ISO 22301: 2012	ISO 28000: 2007	ISO 31010: 2019	ISO 31000: 2018	ISO 37001: 2016	ISO 39001: 2012	ISO 28000: 2007	ISO 22301: 2012	ISO 20000-1: 2018	ISO 14971: 2019	ISO 27005: 2018	ISO 62366-1: 2015	Occurrence, Definition of RA	SR-A	
16	Analysis (in general) is the process of examining data to reveal relationships, patterns, and trends. This can mean the use of statistical operations, including information from other similar organizations, to help draw conclusions from the data. This process is most often associated with measurement activities																							1	DeFN
17	The organization shall analyze and evaluate the identified risks																							1	
18	The organization shall undertake regular bribery risk assessment(s), which shall analyze, assess, and prioritize the identified bribery risks																							1	
19	RA should consider factors such as: the likelihood of events; the nature and magnitude of consequence; complexity and connectivity; time-related factors and volatility; the effectiveness of existing controls; sensitivity and confidence levels																							1	DeFN
20	Highly uncertain events that can have severe consequences can be difficult to quantify, in such cases using a combination of techniques generally provides greater insight																							1	

(Continued)

Table IV. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk Analysis (RA)	ISO 9001: 2015	ISO 14001: 2015	ISO 22000: 2018	ISO 45001: 2018	ISO 13485: 2016	ISO 50001: 2018	ISO 20000- 22301: 2012	ISO 28000: 39001: 2012	ISO 31000: 37001: 2016	ISO 31010: Guide IEC 27005: 2019	ISO 73: 2009	ISO 14971: 62366- 1: 2015	IEC Occurrence, Definition of RA
21	For analyzing interactions and dependencies between risks, it can be useful to create a causal model that incorporates the risks in some form													1
22	The outcomes from RA provide an input to decisions that need to be made and actions that are taken													1
23	Consequence analysis can vary from a description of outcomes to detailed quantitative modeling or vulnerability analysis													1
24	The magnitude of consequences can be expressed quantitatively as a point of value or a distribution													1
25	The types of consequences to be analysed should have been decided when planning the assessment													1
26	Consequences might change over time													1
27	Likelihood can refer to the likelihood of an event or a likelihood of a specified consequence													1
28	There are usually many interactions and dependencies between risks to be analyzed													1
29	Those analyzing risk should understand the uncertainties in the analysis													1

(Continued)

Table IV. (Continued)

No.	Risk Terminology in ISO Standards/Definition and Description of Risk Analysis (RA)	ISO 9001: 2015	ISO 14001: 2015	ISO 27001: 2013	ISO 22000: 2018	ISO 45001: 2018	ISO 50001: 2018	ISO 9001: 2018	ISO 13485: 2016	ISO 20000- 22:301: 2012	ISO 28000: 39001: 2007	ISO 31010: 37001: 2018	ISO 31000: 31010: 2019	ISO Guide 73: 27005: 2018	ISO 14971: 62366- 1: 2019	IEC 60601- 1: 2015	IEC 62366- 1: 2015	Occurrence, Definition of RA	
30	Process to comprehend the nature of risk and to determine the level of risk																	1	Def-N
31	RA provides the basis for risk evaluation and decision about risk treatment																	1	(Def-B)
32	RA can be qualitative or quantitative, or a combination of these																	1	
33	Qualitative analysis is often used first to obtain general indication, later it can be necessary to undertake more specific or quantitative analysis on major risks																	1	
34	Qualitative RA uses a scale of qualifying attributes																	1	
35	Quantitative RA uses a scale with numerical values																	1	
36	To analyze all risks of a medical device, the manufacturer needs to consider carefully the full range of use scenarios and associated factors that could lead to harm																	1	
Total number of risk analysis descriptions per standard:		2	1	1	0	1	1	0	0	1	0	1	2	9	3	7	7	1	37

Note: "x": appears in the relevant ISO standard; " " : does not appear in the relevant ISO standard; "Def-N/B": in accordance with Narrow/Broader definition in SRA glossary, see Subsection 2.1; "(Def-N/B)": somewhat in line with SRA glossary.

strong limitations in analyzing many types of real-life systems, particularly complex systems that are characterized by large uncertainties and the potential for surprises. Resilience is therefore relevant for the state-of-the-art risk management.

The second paper is from Oughton *et al.* (2019). They discuss a general risk assessment framework with focus on critical infrastructure systems. The authors discuss the need for a rigorous risk assessment framework to analyze the potential socioeconomic impact of space weather on high-voltage electricity transmission networks. They provide a framework to assess failure resulting from geomagnetic disturbances. Analyzing risk in critical infrastructure systems and analyzing risk factors like socioeconomic impact requires a multidisciplinary approach that is relevant for the state-of-the-art risk management.

The third paper is from Montibeller and Winterfeldt (2015). They address the danger of cognitive and motivational biases in risk analysis and decision making. When eliciting model components and parameters from decisionmakers or experts, analysts often face the very biases they are trying to help overcome. When these inputs are biased, they can seriously reduce the quality of the model and resulting analysis. Some of these biases may be due to faulty cognitive processes, others due to motivations for preferred analysis outcomes. Behavioral decision research demonstrates that people's judgment and decisions are subject to numerous biases. Considering human behavior, culture and ethics are relevant for state-of-the-art risk management since risk and decision analysis are meant to improve judgment and overcome biases. Montibeller and Winterfeldt consider it surprising how little attention the biasing issues have received in decision and risk analysis.

The fourth paper is from Rozell (2018). He discusses the importance of ethical foundations of risk analysis; an aspect of increasing importance when making controversial decisions. Rozell points out that no normative theory is perfect, and the ethical underpinnings of any risk management decision can be a potential source of controversy. Although an ethical framework must eventually be chosen as a basis for assessment, recognition of the weaknesses of any approach is necessary if an honest and useful risk analysis is to be presented. Being aware of weaknesses adds to necessary knowledge and understanding of risk and makes the risk analysts less likely to make the naive assumption that their methods will be universally accepted as fair and objective. Risk

management decision should address potential shortcomings, both methodological and philosophical, to maximize acceptance. Rozell points out weaknesses in traditional formal methods in the field of risk analysis. Acknowledging such weaknesses and finding ways to improve the traditional methods is important for state-of-the-art risk management. Rozell assumes idealized, objective, and quantitative analysis at the expense of hardly quantifiable but important risk characteristics. His view is that objective narrow assessments are useful, but not necessarily superior to subjective broad assessments.

The fifth paper is from Alderson *et al.* (2015). They address risk and resilience in systems of interacting components. They propose a definition of infrastructure resilience that has recently become an important topic. This definition is tied to the operation of such systems that can be objectively evaluated using quantitative models. They point out that in practice, modern infrastructure systems consist of humans and autonomous "agents," like monitoring systems and feedback controllers that make decisions to guide the overall system behavior. Alderson *et al.* also point out that modeling the behavior of an infrastructure system in terms of a constrained optimization problem does not necessarily mean that the real operation of the system is truly optimal. Their way to model such systems is rather to identify the essential structural features, defined in terms of the problem's objectives and constraints. Their research demonstrates that methods to model, often critical, infrastructure systems are an important issue for the state-of-the-art risk management.

The differentiation between safety and security is the topic of Amundrud, Aven, & Flage (2017). They discuss how the definition of security risk can be made compatible with safety definitions. In their paper, they describe the risk concept as generic and independent of applications in the sense that whether addressing safety, security, or other areas, we face some potential risk sources or events (threats) that may lead to consequences in terms of something that humans value. In the risk science, the term risk is defined in relation to the consequences of future activity (in a wide sense) with respect to something that humans value. The focus is often on negative, undesirable consequences. At least one outcome is considered negative or undesirable (Society for Risk Analysis Glossary, 2018). Thus, risk management is defined as activities to manage risk, such as prevention, mitigation, adaptation, or sharing. It often includes tradeoffs between benefits and costs of risk reduction

and choice of a tolerable risk. Amundrud et al. (2017) address the difference of risk definition in safety settings on one hand and security settings on the other hand. In safety settings, risk is commonly defined as a combination of consequences and associated probabilities or uncertainties. In security settings, risk is commonly defined as a combination of asset/value, threat, and vulnerability. Amundrud et al. (2017) argue that it is not necessary to define risk differently in these two settings. Accordingly, for state-of-the-art risk management, the same approaches should apply to risk modeling, risk analysis and risk management, whether in case of safety or security.

Modern sociotechnical systems are examples of coherent systems where human factors and emerging behavior have become increasingly important for state-of-the-art risk management. One of the first engineers to acknowledge the behavior of such systems and integrate human factors and engineering was Rasmussen (Rasmussen, 1997). He applied his ideas in safety risk area and raised the question whether the models used to analyze accident causation are adequate for the present dynamic society. He described the challenges faced in risk management when modeling a sociotechnical system, characterized by fast technological change. Its environment is increasingly aggressive and competitive with varying regulatory practices and public pressure. He suggested cross-disciplinary research and creation of a cross-disciplinary research community that can cope with complex long-term research issues without the constraints of academic institutes and their focus on short-term tenure strategies.

Rasmussen's contribution to the state-of-the-art risk management influenced Leveson (Leveson, 2011a). Leveson applied Rasmussen's ideas beyond human factors to influence the way that engineers approach the entire engineering process for complex, safety-critical sociotechnical systems. She addresses interactive complexity (interaction between system components), dynamic complexity (changes over time), decompositional complexity (structural composition not consistent with functional decomposition), and nonlinear complexity (where cause and effect are not related in a direct or obvious way). Leveson uses systems theory to develop a general causality model of complex systems called Systems-Theoretic Accident Model and Processes (STAMP) (Leveson, 2004; Leveson, 2011b). Based on the STAMP causality model, Leveson also describes a new approach to hazard and risk analysis, called

System-Theoretic Process Analysis (STPA). Leveson proposes the new STAMP method to identify system-specific leading indicators (Leveson, 2015). The intent of this method is to provide guidance in designing a risk management structure to generate, monitor and use the results. Rather than using classic probabilistic risk methods, assumptions and their vulnerability are used as the basis for identifying leading indicators. Both Leveson's causality models and methods to identify leading indicators can be applied equally within safety and security areas and address important issues for state-of-the-art risk management.

In their study on workplace safety, Carayon et al. (2015) advocate a sociotechnical systems approach describing the complex multilevel system factors that contribute to workplace safety. From the literature on sociotechnical systems, complex systems, and safety, they develop a sociotechnical model of workplace safety with concentric layers of the work system, socio-organizational context, and the external environment. They point out particular limitations of ongoing efforts: "First, risk management models that underlie scientific and professional approaches have only a limited ability to address latent and/or emergent risks and a restricted capacity to address the complexity of current and proposed work systems. Second, the focus on the individual worker loses many important phenomena when viewed from the broader sociotechnical systems perspective." Carayon et al. propose a shift in the analysis toward the sociotechnical system level. Such shift will incorporate human interdependencies relative to important social and technical elements. Meaningful advances in safety can be made if the analysis is shifted to the sociotechnical system level and methodologies are expanded so the resilience and the adaptive role of people (workers) in creating safety can be revealed. The human role in sociotechnical systems, both for their resilience of systems and safety of people, is an important issue for the state-of-the-art risk management.

Aven and Zio (2014) address foundational issues in risk assessment and risk management. Foundational issues are important for state-of-the-art risk management and one of the reasons why SRA was founded. Aven and Zio discuss the needs, obstacles, and challenges for the establishment of a renewed, strong scientific foundation for risk assessment and risk management suited for the current and future technological challenges. Their article provides

reflections on the interpretation and understanding of the concept of “foundations of risk assessment and risk management” and the challenges therein. Aven and Zio point out that the risk assessment and risk management fields suffer from a lack of clarity on many key scientific pillars. There is a lack of consensus on even basic terminology and principles, lack of proper scientific support, and justification of many definitions. Perspectives adopted lead to an unacceptable situation for operatively managing risk with confidence and success. There are many reasons why it is difficult to establish a strong scientific platform for risk assessment and risk management. One is that the risk field is strongly multidisciplinary, thus involving many communities of scientists and practitioners. Therefore, one of Aven and Zio’s main recommendation is that different arenas and moments for discussion are needed to specifically address foundational issues in a way that embraces the many disciplinary communities involved. This means that much collaboration is needed by those involved. Awareness of the importance of the contribution to state-of-the-art risk management can hopefully be a driving force.

Zio (2016) provides a systematic view on the problem of vulnerability and risk analysis of critical infrastructures. He addresses the complexity of critical infrastructure systems, composed of many components interacting in a network structure. Risk associated with such systems is known to be an important issue for the state-of-the-art risk management. Most often, the components are physically and functionally heterogeneous, and organized in a hierarchy of subsystems that contributes to the system function. This leads to both structural and dynamic complexity. Protecting critical infrastructure requires modeling its component fragilities under different hazards and then analyzing their system-level risk and vulnerability. Zio emphasizes the importance of the framework of vulnerability and risk analysis, and that it is examined in relation to its application for the protection and resilience of critical infrastructures. He argues that the complexity of these systems is a challenging characteristic, which calls for the integration of different modeling perspectives and new approaches of analysis.

Carreras *et al.* (2014) write about complex dynamics of interdependent cascading infrastructure systems. They point out that real infrastructure systems typically have an additional layer of complexity. Their heterogeneous coupling to other infrastructure systems can cause a failure in one system to propagate to other systems. Therefore, infrastructure sys-

tems must be modeled through a network with complex system dynamics that has already been stated to be important for the state-of-the-art risk management.

Holovatch *et al.* (2017) address specific time-dependent interactions within complex systems. They manifest rich, nontrivial, and unexpected behavior and state that the study of complex systems forms a new interdisciplinary research area that cuts across physics, biology, ecology, economics, sociology, and the humanities. Again, interdisciplinary and collaborative work is needed to capture issues in state-of-the-art risk management.

Dekker *et al.* (2011) address the complexity of failure and implications of complexity theory for safety investigations. In complex systems, there is no linear relationship between behavior and system-level outcomes. When accidents are seen as complex phenomena, there is no longer an obvious relationship between the behavior of parts in the system and system-level outcomes. Instead, system-level behavior emerges from the multitude of relationships and interconnections deeper inside the system. Risk analysis methods (investigations) that embrace complexity must therefore stop looking for only causes of failure or success. Instead, multiple narratives from different perspectives inside the complex system must be gathered, which may give partially overlapping and partially contradictory accounts of how emergent outcomes come about. The complexity perspective dispenses with the notion that there are easy answers to identify and manage risk associated with complex systems events. All these factors, related to complex systems, are issues in state-of-the-art risk management.

The examples of risk science contributions reviewed in this article describe various challenges, recent developments, and issues that are important for state-of-the-art risk management and risk analysis. The literature confirms the importance and challenges of risk analysis in complex systems. There is a call for new risk analysis methods, new risk models to capture the complex behavior and interconnection of individual time-dependent factors and interactions between people and systems. The results can be summarized to:

- (1) There is need for risk models to capture (nonlinear) functions of complex and critical systems and system interactions (Alderson *et al.*, 2015; Carayon *et al.*, 2015; Carreras *et al.*, 2014; Dekker *et al.*, 2011;

- Holovatch et al., 2017; Leveson, 2011a, 2011b; Rasmussen, 1997; Zio, 2016).
- (2) New approaches, methods, and techniques are needed to capture and analyze risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems (Alderson et al., 2015; Carayon et al., 2015; Carreras et al., 2014; Dekker et al., 2011; Holovatch et al., 2017; Leveson, 2011a, 2011b; Rasmussen, 1997; Zio, 2016).
 - (3) Risk analysis methods need to increase relevant knowledge (Aven, 2019; Aven & Ylönen, 2019; Dekker et al., 2011; Montibeller & Winterfeldt, 2015; Oughton et al., 2019; Rozell, 2018; Zio, 2016).
 - (4) Cross-disciplinary (interdisciplinary) work is needed to analyze and understand risk in sociotechnical systems (Aven & Zio, 2014; Holovatch et al., 2017; Montibeller & Winterfeldt, 2015; Oughton et al., 2019; Rasmussen, 1997; Rozell, 2018).
 - (5) There is need for strong scientific foundation and framework for risk management suited for current and future challenges (Aven, 2019; Aven & Ylönen, 2019; Aven & Zio, 2014; Oughton et al., 2019; Zio, 2016).
 - (6) The relationship and difference between risk and resilience needs more research (Alderson et al., 2015; Aven, 2019; Carayon et al., 2015; Zio, 2016).
 - (7) Clear risk terminology is needed (Amundrud et al., 2017; Aven & Zio, 2014).
 - (8) Clear ethical framework is needed as a basis for risk assessment and decision making (Rozell, 2018).
 - (9) Definitions of and the effects of not differentiating between safety and security needs to be investigated and clarified (Amundrud et al., 2017).
 - (10) Identification of leading risk indicators is needed (Leveson, 2015).

2.2. Literature on ISO Standards

When it comes to literature on ISO standards, it must be noted that ISO regularly updates its standards. Therefore, much of the literature on older versions of ISO standards is not relevant. The papers reviewed in this section were found through searching Google Scholar for “risk management in ISO standards” from 2009 and “ISO 31000 2018 risk

management review” from 2018. Most of the papers found in the first search focus on the application of ISO 31000, first published in 2009 and then revised in 2018. Then principles of risk management were reviewed, and greater emphasis put on leadership by top management to ensure that risk management is integrated into all organizational activities, starting with the governance of the organization. Greater emphasis is also now on the iterative nature of risk management, drawing on new experiences, knowledge, and analysis for the revision of process elements, actions, and controls at each stage of the process. Most of the papers (Aven, 2011; Aven & Ylönen, 2019; Barafort, Mesquida, & Mas, 2017; Leitch, 2010; Olechowski, Oehmen, Seering, & Ben-Daya, 2016; Purdy, 2010;) reviewed in this section concern the ISO 31000:2009 version, others the 2018 version (Parviainen, Goerlandt, Helle, Haapasaari, & Kuikka, 2021; Silva Rampini, Takia, & Berrsaneti, 2019). The changes in the standard do not affect this review. Some papers focus on risk management in information technology (IT) based on ISO standards, and integration of many ISO standards in one management system. Some authors discuss the benefits of applying ISO standards, while others are critical of the standards and their lack of scientific basis.

According to the paper of Aven and Ylönen (2019), previously mentioned in Subsection 2.1., the current trend of using standards represents a serious threat to the advancement of the risk field. The main reason is that standards lack scientific basis. The authors take ISO 31000 as an example and criticize inconsistency in terminology and the process for developing and improving the standards. Their conclusion is that measures need to be taken to create broader and more scientifically based arenas for guiding risk and safety analysis and management practices.

Rampini et al. (2019) analyze academic interest in risk management in relation to critical success factors through the use of ISO 31000:2018. Their analysis was carried out with samples of documents from 2008 to 2018. Rampini et al. (2019) argue that the field would benefit from further research on topics concerning ISO 31000 and quality management, for example, on the relationship between risk and performance management. They suggest exploring the shared role of ISO 31000 and its application from different perspectives.

Parviainen et al. (2021) explore how Bayesian risk models can be aligned with the ISO 31000:2018 framework by offering a flexible approach to integrate various sources of probabilistic knowledge.

In their opinion, the ISO 31000 standard provides a comprehensive framework for contextualizing, assessing, evaluating, and treating risks. Their conclusion is that the appropriate risk analysis models help to implement the ISO 31000 risk management framework in practice.

Barafort *et al.* (2017) present a comparison of how risk management is addressed in several ISO standards with regard to IT and security. Based on ISO 31000, they compare risk management activities in five MSSs: ISO 9001, ISO 21500, ISO/IEC 20000-1, and ISO/IEC 27001. Their paper reveals high interest and business need for solid basis to improve, coordinate, and interoperate risk management activities in IT settings for various purposes related to quality management, project management, IT service management, and information security management. The paper shows that organizations heavily rely on the ISO standards to manage their risk, a growing need for integration of various standards requirements, and clear and uniform definition of risk terms.

Purdy (2010) discusses the consensus-driven development process of ISO standards. He reviews ISO 31000:2009 together with ISO Guide 73:2009 and acknowledges the fact that these publications support a new, simple way of thinking about risk and risk management. ISO's intention with these two publications was to begin the process of resolving the many inconsistencies and ambiguities that had existed, and still exist, between many different approaches and definitions within the risk management field. Although Purdy is positive about this effort, he points out that there is room for improvement.

Aven (2011) conducts a critical review on the ISO Guide 73:2009 and the risk concept. The ISO guide provides foundation of many ISO standards on risk management, including ISO 31000. Its quality is therefore critical. Aven argues that the guide fails in several ways to produce consistent and meaningful definitions of many of the key concepts covered. His conclusion is that the definition of the term "risk" is unclear and that it offers different interpretations. He also concludes that it is not possible to establish a consistent conceptual framework for risk assessments and risk management based on the terminology introduced in the ISO documents. He states that many reformulations are required and suggests some main changes.

Leitch (2010) is more skeptical than Purdy about ISO's attempt to develop ISO 31000 as a general

standard for managing all risks everywhere. He discusses the consequence of publishing such a standard that certain ideas about risk and its management get a boost in credibility and prominence while others loose out. Leitch writes about risk terminology in ISO 31000:2009, which is the same in the latest version published in 2018. He finds it disappointing. His conclusion is that the standard is unclear, it leads to illogical decisions if followed, it is impossible to comply with, and it is not mathematically based, having little to say about probability, data, and models.

Olechowski *et al.* (2016) present results of an empirical study of the principles of the ISO 31000:2009 via a large-scale survey of engineering and product development practitioners. The principles of ISO 31000 have been streamlined and slightly changed in version 2018, but they are essentially the same. The finding of Olechowski *et al.* (2016) suggests that the ISO principles, applied at a high level, have potential to be the basis for shared understanding of best practice and to catalyze the professionalization of project risk management. They believe that the principles can form a foundation on which a shared understanding of best practice and an increase in the collective competence can be built. Therefore, they propose the principles as an alternative to a single rigid standard. Making ISO 31000 only to principles and omit detailed guidance is, however, not in line with ISO's purpose for the standard. The framework and process of a risk management system is meant to provide necessary support for such a system. The guidelines in ISO 31000 are furthermore meant to support and complement various ISO MSSs that form the basis for accredited certification. According to Leitch and Olechowski *et al.*, the creation process for ISO 31000 is largely unknown, including the origin of the risk management principles that are presented. Their roots seem not to be based on recent risk science but on the Australian and New Zealand standards (AS/NZS 4360:2004 and AS/NZS HB436:2004).

The review of the literature on ISO standards in Subsection 2.2 confirms the importance and challenges of risk management in present-day sociotechnical systems, like in Subsection 2.1. The literature shows that it is difficult to standardize the assessment criteria for something that is intangible, for example, Aven (2011) and Olechowski *et al.* (2016). It is important to understand the concept of risk management, as set out in Subsection 2.1. There is a limit to how well standards can reflect the concept of risk management. The use of standards involves the assessment

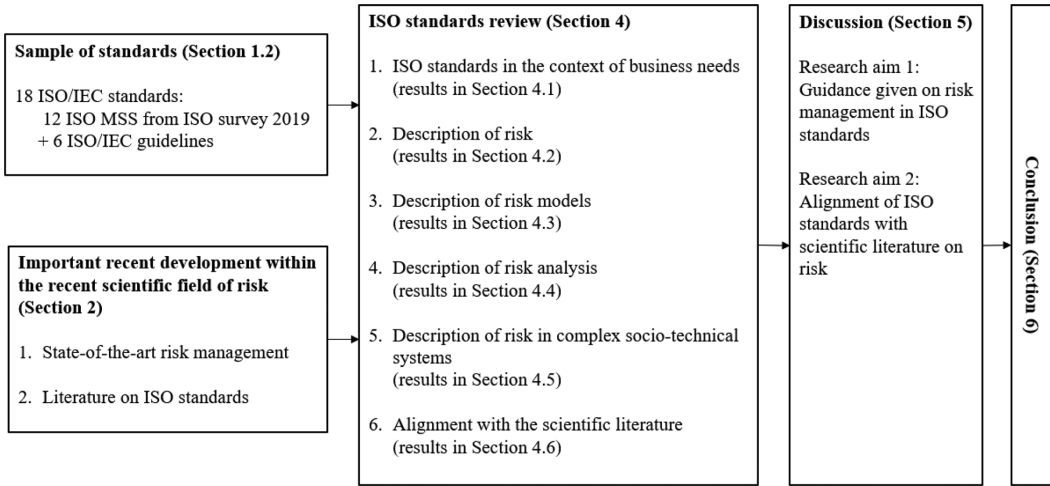


Fig 1. Research Methodology.

of the usefulness of models or technologies that are considered to adequately identify risks. The results of the review of literature on ISO standards can be summarized to:

- (1) It is important that risk terms are well-defined, clear, and uniform in all ISO standards (Aven, 2011; Aven & Ylönen, 2019; Barafort et al., 2017; Leitch, 2010; Purdy G., 2010).
- (2) Organizations heavily rely on ISO standards to manage their risk (Aven & Ylönen, 2019; Barafort et al., 2017; Purdy G., 2010; Silva Rampini et al., 2019).
- (3) ISO standardization work is important because it is based on shared understanding and best practices, but that is, however, not enough for future development of the standards (Olechowski et al., 2016; Purdy G., 2010).
- (4) Collaboration and interdisciplinary work of risk specialists is needed to develop ISO standards that cover risk management (Aven & Ylönen, 2019; Silva Rampini et al., 2019).
- (5) ISO standards are missing out on risk frameworks and risk models (Aven, 2011; Leitch M., 2010).
- (6) It is not enough to have market forces controlling the development of ISO standards, they must be based on risk science (Aven & Ylönen, 2019).

3. RESEARCH METHODOLOGY

In this study 18 ISO standards (see Table II) were reviewed with regard to business needs for risk management and risk issues found in Section 2: (1) context of business needs; (2) description of risk; (3) description of risk models; (4) description of risk analysis; (5) description of risk in complex sociotechnical systems; (6) alignment with scientific literature. Fig. 1 describes the research methodology and its individual steps in a schematic way, also reflecting the structure of this article.

4. RESULTS

Results of this study are presented in the following six subsections. They were obtained in the time frame 2014–2020. During this period, all changes to the ISO standards in the ISO survey and the guidelines regarding risk management were reviewed annually and changes recorded. The changes demonstrate increasing focus on risk management in ISO standards. The results are presented in tables, discussed, and conclusions drawn.

4.1. ISO Standards in the Context of Business Needs

ISO standards development since 2014 confirms increasing focus on risk management in most

business sectors. The findings of this study can be summarized as follows:

- (1) Results from ISO survey 2019 in Table I show that risk management is becoming a vital part of all ISO-certified management systems. All the MSSs in the survey require risk management in some way, which reflects business needs.
- (2) In 2015, when risk-based thinking became a requirement in ISO 9001 and ISO 14001, risk management formally became a part of most of the ISO-certified management systems in the world.
- (3) All ISO MSSs refer to ISO risk management guidelines except ISO 28000. The explanation could be that the standard was published in 2007 and has not been updated since.
- (4) Eight of 12 ISO MSSs refer to ISO 31000.
- (5) Seven of 12 ISO MSSs refer to ISO Guide 73.

4.2. Diversity in the Risk Terminology Across ISO Standards

The term “risk” is a keyword in the context of risk management, now addressed in many ISO standards as already presented in this article. To help users work with many standards, ISO has published a handbook with guidelines on how to integrate multiple management standards into a single management system within an organization (International Organization for Standardization, 2018f). Its aim is to support organizations and assist them in maintaining a sustainable business model through changing environments. This means that organizations should be able to add new emphases in their management systems by adding new and different standards as needed.

For this concept to work well, terminology must be clear and easy to understand. This can be a challenge, since many of the industries have developed their own risk terminology based on tradition, culture, and literature in certain areas. The term “risk” itself is a word that can have a different meaning, depending on the context. Table III shows the descriptions of risk found in the ISO standards. The table has 22 columns. First two columns of the table show line numbers and all the descriptions of risk found in the 18 ISO standards reviewed. The following 18 columns indicate in which of the 18 standards the description can be found. The marker “x” means that the description can be found in the respective

standard. The total number of occurrences, that is, in how many standards where description appears, is also shown. The last column shows which definitions/descriptions are in line with SRA glossary, see Subsection 2.1. The bottom line of the table shows the total number of different risk descriptions found in every standard.

Table III shows that the term “risk” is described in 44 different ways. This can be summarized as follows:

- (1) The risk terminology in the ISO standards is not based on risk science.
- (2) Definitions/descriptions of risk in ISO standards are not in line with SRA glossary, except for those in lines no. 23, 41, and 42, which are in line with SRA’s risk description no. 1 (Subsection 2.1). Definitions/descriptions in lines no. 2, 5, 7, 19, 21, 27, 28, 32, and 35 are somewhat in line with SRA glossary.
- (3) IEC 31010, IEC 31010, and ISO 37001 are most descriptive of risk.
- (4) ISO standards describe (and define) risk in diverse ways and some standards are more generic than others.
- (5) In most standards, risk is seen as a harmful thing. However, in some (ISO 9001, ISO 14001), risk is associated with opportunities or positive effects.
- (6) The meaning of risk must be read and understood from the context, for example, usability risk for medical devices.
- (7) The most used description of risk is “Risk can/must be managed/controlled/addressed.” It appears in 14 of 18 standards, not, however, in the ISO Guide 73.
- (8) The description (definition) of risk as “the effect uncertainty has on objectives” appears in 11 of 18 standards.
- (9) Only four of 44 risk descriptions are identical in more than half of the standards.
- (10) Many ISO standards contain similar description of risk, but no two standards in this study contain the same set of descriptions in all aspects.
- (11) Five ISO standards (ISO/IEC 27001, ISO 37001, ISO 31000, IEC 31010, ISO 14971) describe risk in the context of magnitude and different levels of risk.
- (12) Only one standard (IEC 31010) describes risk as an item in a risk register.

- (13) Three standards (ISO/IEC 27001, ISO 31000, IEC 31010) describe risk as “owned” by someone, that is, someone is made responsible for treating the risk, which is important when it comes to taking the initiative.
- (14) Three standards (ISO 37001, ISO 31000, IEC 31010) describe risk as a cultural subject where perception depends on cultural background.
- (15) Three standards (ISO/IEC 27001, ISO 31000, IEC 31010) associate risk with vulnerability.

4.3. Little Mention of Risk Models in ISO Standards

Based on the review of the ISO standards in this study, the results are as follows:

- (1) There is little mention of risk models in the 18 ISO standards reviewed, except for IEC 31010.
- (2) IEC 31010 gives a general description of how to develop and apply a model: “A model is an approximate representation of reality. Its purpose is to transform what might be an inherently complex situation into simpler terms that can be analyzed more easily.”
- (3) Only IEC 31010 addresses interactions between risks, humans, and systems in connection with risk models.
- (4) IEC 31010 mentions risk models in an overview of different risk assessment techniques in Annex B, with references to some of the techniques.
- (5) ISO 31000 mentions models for examination of the organization’s context, and open systems model to fit multiple needs and context in ISO 31000. Other standards mention management system models or Plan-Do-Check-Act model (International Organization for Standardization, 2015a; International Organization for Standardization, 2015b).
- (6) Despite ISO Guide 73 providing the “basic vocabulary to develop common understanding on risk management concepts and terms” for ISO standards, there is no definition or description of “risk model” in the guide.
- (7) In ISO/IEC 27005 it says that the quality of risk analysis depends on the models used, and by modeling outcomes of events, consequences, and business impacts can be determined. There is no mention of risk models.

4.4. Lack of Guidance on Doing Risk Analysis in ISO Standards

Risk analysis is a key element within the risk management process and all ISO MSSs in ISO survey 2019 except one (ISO 28000:2007) refer to risk guidelines. Table IV shows the descriptions (guidance) on risk analysis found in the ISO standards. The table has 22 columns. First two columns of the table show line numbers and all the descriptions of risk analysis found in the 18 ISO standards reviewed. The following 18 columns indicate in which of the 18 standards the description can be found. The marker “x” means that the description can be found in the respective standard. The total number of occurrences, that is, in how many standards that description appears is also shown. The last column shows which definitions/descriptions are in line with SRA glossary (in either narrow or broad sense), see Subsection 2.1. The bottom line of the table shows the total number of different risk analysis descriptions found in every standard. The overview of risk assessment techniques in the annexes of IEC 31010, which in some places mention risk analysis in relation to a specific technique, is not included.

Table IV shows that risk analysis is defined/described in 36 different ways in the ISO standards. Only two standards apply the same definition/description of risk analysis, as can be seen in line no.10. The results of this review can be summarized as follows:

- (1) There is no uniform definition/description of risk analysis in the ISO standards.
- (2) Definitions/descriptions of risk analysis in ISO standards are not in line with SRA glossary, except for those in lines no. 3, 8, 16, 19, and 30, which are in line with the SRA’s narrow definition of risk analysis (Subsection 2.1). Definitions in lines no. 1, 7, 9, 10, 15, and 31 are somewhat in line with SRA glossary, either the narrow or the broader definition.
- (3) Most definitions/descriptions and guidance on risk analysis can be found in IEC 31010, ISO/IEC 27005, and ISO 14971.
- (4) IEC 31010 specifically deals with risk assessment techniques. It contains two annexes with an overview of some traditional risk assessment techniques that can be applied during steps of the ISO 31000 risk management process. It describes factors to consider when selecting technique(s) for a particular purpose.

Reminder is given that care should be taken in selecting the appropriate technique. A description of techniques is given in two annexes and references are given to documents.

- (5) IEC 31010 addresses the analysis of type, magnitude, consequences, likelihood, interactions, and dependencies of risk, as a way to understand consequence and likelihood of risk.
- (6) IEC 31010 describes the difference between qualitative and quantitative methods. ISO/IEC 27005 also contains a short description of qualitative and quantitative methods. Other standards do not mention this.
- (7) In both ISO 9001 and ISO 14001, there is no requirement for formal methods or a documented risk management process.
- (8) There is no description of risk analysis in ISO 22000, ISO 50001, ISO 20000-1, ISO 28000, and ISO 39001.

4.5. Little Mention of Risk in Complex Sociotechnical Systems in ISO Standards

The literature review (Subsection 2.1) shows that there are many risk issues that are important for the state-of-the-art risk management. There are also many terms used in the scientific literature to describe the challenge of managing risk in modern systems. Issues and terms like “complex systems,” “sociotechnical systems,” “causal relation,” and “emergent behavior” are frequently used (Alderson *et al.*, 2015; Aven, 2019; Aven & Zio, 2014; Carayon *et al.*, 2015; Carreras *et al.*, 2014; Dekker *et al.*, 2011; Holovatch *et al.*, 2017; Leveson, 2015; Leveson, 2004; Leveson, 2011b; Montibeller & Winterfeldt, 2015; Oughton *et al.*, 2019; Rasmussen, 1997; Rozell, 2018; Zio, 2016). Based on the review of the chosen ISO standards, the results are as follows:

- (1) There is little mention of risk associated with complex sociotechnical systems in ISO standards. As an example, ISO 31000 only mentions that risk analysis should consider factors such as complexity and connectivity. IEC 31010 mentions complex systems, dependences, and interconnected risks.
- (2) The ISO standards assume a linear causal relationship, not one associated with complexity and emergent behavior. IEC 31010 addresses causal relationships and connections but does not address nonlinearity.

- (3) There is no mention of lack of linear causal relations, which is typical of complex sociotechnical systems.
- (4) There is no mention of emergent behavior. There is, however, mention of “emerging good practice and guidance” in ISO 22301, “identifying emerging risks” in ISO 31000, “re-emerging threats” in ISO/IEC 27005, and “human behavior” as a source of risk in IEC 31010.
- (5) Examples of risk assessment techniques in Annex B of IEC 31010 mention “causal relationship.” There is, however, no mention of the predominance of emergent behavior and corresponding lack of linear causal relations in complex sociotechnical systems.
- (6) Although ISO 14971 and IEC 62366-1 aim at making medical devices safe and managing risk in both production and use, they reach neither emergent behavior nor user behavior. Both standards mention behavior only once, despite behavior being an important element in the application of many medical devices.

4.6. ISO Standards Not Aligned with Scientific Literature on Risk Management

ISO’s aim is to create documents that provide requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that materials, products, processes, and services are fit for their purpose³. ISO states that the standards and guidelines are made by experts from both industry and academia⁴. The measure of the quality of standards regarding risk management must logically include how well they align with scientific literature and state-of-the-art risk management. In this study, the ISO standards were reviewed with regard to important recent developments within the scientific field of risk. In view of the points summarized in Subsection 2.1, the results are as follows:

- (1) Need for risk models to capture (nonlinear) functions of complex and critical systems and system interactions:

There is very little mention of complex and critical systems in ISO standards, and neither mention of importance nor description of how to model such systems. There is no

³<https://www.iso.org/standards.html>

⁴<https://www.iso.org/developing-standards.html>

mention of systems theory in the standards, even though it is state-of-the-art in the literature. There is also no reference to scientific literature on this.

- (2) Need for approaches, methods, and techniques to capture and analyze risk arising from complex interactions and emergent behavior that is inherent in present-day sociotechnical systems:

There is little description of this in ISO standards. IEC 31010 mentions techniques to analyze “risk of complex systems.” There is no reference to scientific risk literature, except for reference to literature on risk assessment techniques (handbooks), albeit not scientific risk literature.

- (3) Risk analysis methods that increase relevant knowledge:

The description of risk analysis in ISO standards is inadequate and not based on risk science.

- (4) Cross-disciplinary (interdisciplinary) work is needed to analyze and understand risk in sociotechnical systems:

ISO states that their standards are made by experts from both industry and academia. There is, however, no mention of risk in sociotechnical systems. The ISO standards are not aligned with scientific literature on these systems, and they do not reflect collaboration with academic organizations and experts in risk science (e.g., SRA).

- (5) There is need for strong scientific foundation and framework for risk management, suited for current and future challenges:

Scientific foundation and framework for risk management is missing in ISO standards.

- (6) The relationship and difference between risk and resilience needs more research:

One of the features of risk science is the distinction between risk and resilience, where risk addresses scenarios that are likely to occur or can be anticipated, while resilience assumes that failures will occur due to unforeseen circumstances. In this relatively new phase in the risk science field, one can expect that the guidelines and standards will reflect practice in a descriptive, not a normative, sense. This descriptive sense may explain why

the definitions of risk concepts do not seem clear. ISO standards need to address these issues.

- (7) Clear risk terminology is needed:

The risk terminology in ISO standards is neither uniform nor science-based. The definition of “risk” and “risk analysis” in ISO standards is different from the SRA risk glossary (Society for Risk Analysis Glossary, 2018). Cross-disciplinary work based on science is needed.

- (8) Clear ethical framework is needed:

This is addressed only indirectly in some ISO standards, in relation to culture.

- (9) Definitions and the effects of not differentiating between safety and security need to be investigated and clarified:

This issue needs clarification in ISO standards, based on risk science.

- (10) Identification of leading risk indicators:

There is no mention of early warning signs and risk indicators in ISO standards.

5. DISCUSSION

The aim of this study was twofold: (1) to investigate and evaluate guidance given in ISO standards on risk management, especially for the critical step of risk analysis; and (2) to investigate how well the standards are aligned with the scientific literature and state-of-the-art thinking on risk.

5.1. First Aim: Guidance Given in ISO Standards on Risk Management

A variety of ISO standards have been reviewed in this study that all have addressed risk management in some way. It is logical that some standards form the basis of risk management, which then other standards refer to and build on. An example of this is ISO Guide 73 that defines risk management vocabulary, ISO 31000 with general guidelines, and IEC 31010 with risk assessment techniques. It is hardly realistic to expect that one “golden standard” for risk management can be created. However, for the standards to be of more help to users, risk terminology should be uniform and consistent in all standards because most organizations use not only one but many ISO standards. When the risk terminology is different, it

can cause confusion. The guidance must be appropriate, and reference must be made to literature to help users find the necessary additional information. To achieve this, the development of ISO standards related to risk management must be based on interdisciplinary collaboration.

A literature review has revealed that the complex sociotechnical systems require new risk analysis methods and techniques, for example, applying systems theory in risk models. It would be helpful for users to have some guidance on these risk issues. ISO standards also need to follow the advancement of technology and societal changes, and they need to address the challenges of modern sociotechnical systems, for example, regarding automation and use of artificial intelligence. The guidance of ISO standards needs to guide users in the right direction in finding solutions and looking for additional knowledge when needed. If the standards are inappropriate, they will not achieve their aim to protect society from harm.

There is a contradiction in having a general and practical standard on risk management, and concurrently wanting it to give detailed guidance on appropriate methods and provide support on risk identification and analysis in complex human–system interaction. ISO 31000 only addresses this kind of risk indirectly by emphasizing the importance of identifying risk and saying that it is important to consider factors like magnitude of risk, complexity, and connectivity. The additional guidance in IEC 31010, with an overview of several risk assessment techniques, fills in some of the gaps. Still missing though is the guidance to help identify and understand the complex interactions and emergent behavior that is inherent in present-day sociotechnical systems. None of the ISO standards are adequate when it comes to managing risk and capturing complex risk concepts in the risk science field. This cannot be expected since standards are based on models of reality that can never fully incorporate all the complexity of real conditions.

5.2. Second Aim: Alignment of ISO Standards with Scientific Literature on Risk Management

Recent literature on risk management describes various risk issues and challenges faced when managing risk in complex sociotechnical systems. Several approaches to systems thinking have been proposed to understand such systems. These approaches may increase system and risk understanding but may still

need to be supplemented with other approaches to adequately support risk management. Better modeling is advocated and qualitative modeling tools with description of systemic behavior are recommended for identification of possible accidents in complex system. The ISO standards do neither address the importance of risk models nor do they describe how to go about creating such models.

The literature confirms the importance of conducting a solid risk analysis in complex sociotechnical systems. This requires more knowledge of risk analysis than can be found in ISO standards. In fact, it requires both expertise in systems functionality and risk analysis methods. It is not within the reach of all companies to hire experts in risk analysis. Therefore, many projects and solutions can be expected to be brought to the market without adequate design, which creates unknown risk that can be difficult to manage. ISO's goal is to produce globally relevant international standards. ISO's strategy is: "ensuring a coherent and credible collection of standards that are used effectively by industry and bring recognized benefits to economies" and "identifying and meeting the changing needs of customers, with a focus on how they would like to use and access ISO standards" (International Organization for Standardization, 2017). Four trends will impact ISO's future strategy: increasing trade uncertainty, changing societal expectations, urgency for sustainability, and digital transformation (Bird, 2019.). Therefore, the emphasis on effective use of standards as well as identification and meeting changing business needs is clear. The quality of standards must be measured against how well they align with scientific literature and state-of-the-art technology. It is a challenge to find one (golden) standard approach to model complex systems and identify their potential risk. It creates tension; complexity makes guidance more desirable, but overly prescriptive guidance may not be flexible enough to accommodate complexity. Over specifications of specific tasks that constitute compliance could even make systems more vulnerable to risk or unforeseen events. This study shows that the ISO standards on risk management are not based on risk science and not aligned with scientific literature. For effective risk management guidance, the ISO standards updating and alignment with the latest scientific literature on risk management is important. This is what industry needs, and this is furthermore ISO's strategic goal in coming years (International Organization for Standardization, 2017; Bird, 2019).

6. CONCLUSIONS AND FUTURE WORK

Despite all the rhetoric and money invested in risk management, businesses too often treat it as merely a compliance issue. Risk management is implemented by setting rules and making sure that all employees follow them. Many such rules do make sense and may reduce harmful risk, but rules-based risk management will not diminish the likelihood or the impact of a disaster (Kaplan & Mikes, 2012). Accredited certification is a way for managers to ensure that all business functions are carried out according to proper processes and procedures, potentially reducing risk. However, this approach does not accommodate the complexity of sociotechnical systems, emergent behavior, and nonlinear causal relations. Thus, better guidelines are required for analyzing and managing risk than those provided in the current ISO standards.

ISO standards have long been the tools used in organizational management and the results of the ISO surveys clearly indicates the growing focus and importance of risk management. Considering the Global Risks Report 2020 (WEF_Global_Risks_Report_2020.Pdf, 2020), a considerable increase in ISO certificates can be expected as a response to increased societal risk and increased requirements for risk management. The numbers of certificates not only indicate the distribution of ISO standards (industry sectors, countries), it is also an indication of how the standards are used (field) and how accessible they are to people who need to apply them. The ISO survey results shows a reduction in certification (and use) of some of the ISO standards (ISO 9001, ISO 14001, ISO 13585, ISO 22301). This indicates the necessity for adjustment of the ISO standards to business needs or else a reduction in general use of ISO standards can be expected. This could mean that other standards organizations, such as the U.S.-based National Institute of Standards and Technology (NIST, n.d.), take a more leading role in the world standardization. This could also mean increasing importance of organizations like SRA (n.d.).

Based on the results of this study, it is hypothesized that certain flaws in risk management will be evident in practice. A follow-up study verifies this through six real-life case study examples. This is the basis for the next paper, soon to be published, where results from the practical cases will be presented.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational models of infrastructure resilience. *Risk Analysis*, 35(4), 562–586. <https://doi.org/10.1111/risa.12333>
- Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 231(3), 286–294. <https://doi.org/10.1177/1748006x17699145>
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13. <https://doi.org/10.1016/j.ejor.2015.12.023>
- Aven, T. (2019). The call for a shift from risk to resilience: What does it mean? *Risk Analysis*, 39(6), 1196–1203. <https://doi.org/10.1111/risa.13247>
- Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability Engineering & System Safety*, 96(7), 719–726. <https://doi.org/10.1016/j.res.2010.12.020>
- Aven, T., & Ylönen, M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? *Reliability Engineering & System Safety*, 189, 279–286. <https://doi.org/10.1016/j.res.2019.04.035>
- Aven, T., & Zio, E. (2014). Foundational issues in risk assessment and risk management. *Risk Analysis*, 34(7), 1164–1172. <https://doi.org/10.1111/risa.12132>
- Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, 54, 176–185. <https://doi.org/10.1016/j.csi.2016.11.010>
- Bird, Kati. (2019). Four trends will impact ISO's future strategy. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2019/09/Ref2436.html>
- Carayon, P., Hancock, P., Leveson, N., Noy, I., Szelwar, L., & van Hootegeem, G. (2015). Advancing a sociotechnical systems approach to workplace safety—Developing the conceptual framework. *Ergonomics*, 58(4), 548–564. <https://doi.org/10.1080/00140139.2015.1015623>
- Carreras, B. A., Newman, D. E., Dobson, I., Lynch, V. E., & Gradney, P. (2014). Thresholds and complex dynamics of interdependent cascading infrastructure systems. In G. D'Agostino & A. Scala (Eds.), *Networks of networks: The last frontier of complexity* (pp. 95–114). Berlin: Springer International Publishing. https://doi.org/10.1007/978-3-319-03518-5_5
- COPOLCO. (2021). ISO - Consumers and Standards: Partnership for a Better World. Retrieved from https://www.iso.org/sites/ConsumersStandards/1_standards.html
- Dekker, S., Cilliers, P., & Hofmeyr, J.-H. (2011). The complexity of failure: Implications of complexity theory for safety investigations. *Safety Science*, 49(6), 939–945. <https://doi.org/10.1016/j.ssci.2011.01.008>
- Holovatch, Y., Kenna, R., & Thurner, S. (2017). Complex systems: Physics beyond physics. *European Journal of Physics*, 38(2), 023002. <https://doi.org/10.1088/1361-6404/aa5a87>
- International Accreditation Forum, Inc. (2020). *International Accreditation Forum—IAF. Find Members, publications & resources*. Retrieved from <https://www.iaf.nu/>

- International Electrotechnical Commission. (2015). *IEC 62366-1:2015, Medical devices—Part 1: Application of usability engineering to medical devices*. Geneva, Switzerland: IEC.
- International Organization for Standardization. (n.d.). *ISO/IEC 27005:2018, Information technology—Security techniques—Information security risk management*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html>
- International Organization for Standardization. (2007). *ISO 28000:2007, Specification for security management systems for the supply chain*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2009). *ISO Guide 73:2009, Risk management—Vocabulary*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2012). *ISO 39001:2012, Road traffic safety (RTS) management systems—Requirements with guidance for use*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2013). *ISO/IEC 27001:2013, Information technology—Security techniques—Information security management systems—Requirements*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2015a). *ISO 9001:2015, Quality management systems—Requirements*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2015b). *ISO 14001:2015, Environmental management systems—Requirements with guidance for use*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2016a). *ISO 13485:2016, Medical devices—Quality management systems—Requirements for regulatory purposes*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2016b). *ISO 37001:2016, Anti-bribery management systems—Requirements with guidance for use*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/50/65034.html>
- International Organization for Standardization. (2017). *ISO Strategy 2016–2020*. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_strategy_2016-2020.pdf
- International Organization for Standardization. (2018a). *ISO 22000:2018, Food Safety Management Systems—Requirements for any organization in the food chain*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/54/65464.html>
- International Organization for Standardization. (2018b). *ISO 31000:2018, Risk management—Principles and guidelines*. Geneva, Switzerland: ISO.
- International Organization for Standardization. (2018c). *ISO 45001:2018, Occupational Health and Safety Management Systems—Requirements with guidance for use*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/37/63787.html>
- International Organization for Standardization. (2018d). *ISO 50001:2018, Energy management systems—Requirements with guidance for use*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/94/69426.html>
- International Organization for Standardization. (2018e). *ISO/IEC 20000-1:2018, Information technology—Service management—Part 1: Service Management System Requirements*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/06/70636.html>
- International Organization for Standardization. (2018f). *The Integrated Use of Management System Standards (IUMSS)*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/publication/10/04/PUB100435.html>
- International Organization for Standardization. (2019a). *ISO 14971:2019, Medical devices—Application of risk management to medical devices*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html>
- International Organization for Standardization. (2019b). *ISO 22301:2019, Security and resilience—Business continuity management systems—Requirements*. Geneva, Switzerland: ISO. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/51/75106.html>
- International Organization for Standardization. (2020). *The ISO Survey*. Retrieved from <https://www.iso.org/the-iso-survey.html>
- ISO & Certification —. (n.d.). ISO Certification and Conformity. Retrieved from <https://www.iso.org/certification.html> (accessed Aug 29, 2021).
- ISO—Management System Standards list (n.d.). Management System Standards List. Retrieved from <https://www.iso.org/management-system-standards-list.html> (accessed Aug 29, 2021).
- Kaplan, R. S. & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, 90(6), 48–60.
- Leitch, M. (2010). ISO 31000 2009 The new INTL standard on risk mgmnt.pdf. *Risk Analysis Journal*, 30(6). Retrieved from <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2010.01397.x/full>
- Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, 42(4), 237–270. [https://doi.org/10.1016/S0925-7535\(03\)00047-X](https://doi.org/10.1016/S0925-7535(03)00047-X)
- Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety*, 136, 17–34. <https://doi.org/10.1016/j.res.2014.10.008>
- Leveson, N. G. (2011a). Applying systems thinking to analyze and learn from events. *Safety Science*, 49(1), 55–64. <https://doi.org/10.1016/j.ssci.2009.12.021>
- Leveson N. G. (2011b). *Engineering a safer world*. Cambridge, MA: The MIT Press. Retrieved from <https://mitpress.mit.edu/books/engineering-safer-world> (accessed Jul 03, 2018).
- Montibeller, G., & von Winterfeldt, D. (2015). Cognitive and motivational biases in decision and risk analysis. *Risk Analysis*, 35(7), 1230–1251. <https://doi.org/10.1111/risa.12360>
- National Institute of Standards and Technology. (n.d.). About NIST (The National Institute of Standards and Technology). Retrieved from <https://www.nist.gov/about-nist>
- Olechowski, A., Oehmen, J., Seering, W., & Ben-Daya, M. (2016). The professionalization of risk management.pdf. *International Journal of Project Management*. Retrieved from 34(8), 1568–1578. <http://www.sciencedirect.com/science/article/pii/S0263786316300631>
- Oughton, E. J., Haggood, M., Richardson, G. S., Beggan, C. D., Thomson, A. W. P., Gibbs, M., ... Horne, R. B. (2019). A risk assessment framework for the socioeconomic impacts of electricity transmission infrastructure failure due to space weather: An application to the United Kingdom. *Risk Analysis*, 39(5), 1022–1043. <https://doi.org/10.1111/risa.13229>
- Parliament and Council of the European Union. (2016). *General Data Protection Regulation 2016/679 of the European Parliament and the Council.pdf* [<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1489504512384&from=en>]. *EUR-Lex Access to European Union Law*. Retrieved from <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1489504512384&from=en>
- Parviainen, T., Goerlandt, F., Helle, I., Haapasaari, P., & Kuikka, S. (2021). Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions. *Journal of Environmental Management*, 278, 111520. <https://doi.org/10.1016/j.jenvman.2020.111520>



- Purdy, G. (2010). ISO 31000:2009—Setting a new standard for risk management. *Risk Analysis*, 30(6), 881–886. <https://doi.org/10.1111/j.1539-6924.2010.01442.x>
- Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, 27(2–3), 183–213. [https://doi.org/10.1016/S0925-7535\(97\)00052-0](https://doi.org/10.1016/S0925-7535(97)00052-0)
- Rozell, D. J. (2018). The ethical foundations of risk analysis. *Risk Analysis*, 38(8), 1529–1533. <https://doi.org/10.1111/risa.12971>
- Silva Rampini, G. H., Takia, H., & Berssaneti, F. T. (2019). Critical success factors of risk management with the advent of ISO 31000 2018—Descriptive and content analyzes. *Procedia Manufacturing*, 39, 894–903. <https://doi.org/10.1016/j.promfg.2020.01.400>
- Society for Risk Analysis Glossary. (2018). *The Society for Risk Analysis*. Retrieved from <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf>
- The Global Risks Report 2020. (2020). *World Economic Forum*. Retrieved from <https://www.weforum.org/reports/the-global-risks-report-2020/>
- The Global Risks Report 2021. (2021). *World Economic Forum*. Retrieved from <https://www.weforum.org/reports/the-global-risks-report-2021>
- The International Electrotechnical Commission. (2019). *IEC 31010:2019, Risk management—Risk assessment techniques*. Geneva, Switzerland: IEC. Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/21/72140.html>
- The Society for Risk Analysis (SRA) (n.d.). About the Society for Risk Analysis. Retrieved from <https://www.sra.org/about-society-risk-analysis>
- Thompson, K. M., Deisler, P. F., & Schwing, R. C. (2005). Interdisciplinary vision: The first 25 years of the society for risk analysis (SRA), 1980–2005. *Risk Analysis*, 25(6), 1333–1386. <https://doi.org/10.1111/j.1539-6924.2005.00702.x>
- WEF_Global_Risks_Report_2020.pdf (n.d.). Retrieved from <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2019/09/Ref2436.html>
- Zio, E. (2016). Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety*, 152, 137–150. <https://doi.org/10.1016/j.ress.2016.02.009>

Article B

Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk

Article

Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk

Svana Helen Björnsdóttir ^{1,*}, Pall Jenson ¹, Saemundur E. Thorsteinsson ², Ioannis M. Dokas ³ 
and Robert J. de Boer ⁴ 

¹ Department of Engineering, Reykjavik University, 101 Reykjavik, Iceland; pallj@ru.is

² Department of Engineering, University of Iceland, 101 Reykjavik, Iceland; saemi@hi.is

³ Department of Civil Engineering, Democritus University of Thrace, 69100 Komotini, Greece; idokas@civil.duth.gr

⁴ Department of Engineering, SDO University of Applied Sciences, 3142 GC Maassluis, The Netherlands; robertjan.deboer@xs4all.nl

* Correspondence: svanahb@ru.is; Tel.: +354-89-99-200

Abstract: The overall aim of this article is to contribute to the further development of the area of benchmarking in risk management. The article introduces a two-step benchmarking model to assess the efficacy of ISO risk management systems. It furthermore aims at verifying its usefulness in terms of finding hidden risk issues and improvement opportunities. The existence of all key elements of an ISO 31000-based risk management system is examined at the beginning of this study. Then, the quality in terms of efficacy of important aspects of the risk management system is examined in more detail with special benchmarks. The application of the model to six ISO-certified organizations follows and reinforces the novelty of this study, which is to combine risk science knowledge with benchmarking theory in the application of ISO risk management standards in organizations. The results show that the benchmarking model developed in this study provides rigor when assessing and evaluating the efficacy of an ISO risk management system. By applying the model, risk issues and risk factors can be found that had not previously been identified. The findings are of importance for risk management, the benchmarking science, and for the development of ISO risk management standards.

Keywords: risk management; benchmarking; ISO risk management systems; ISO 31000



Citation: Björnsdóttir, S.H.; Jenson, P.; Thorsteinsson, S.E.; Dokas, I.M.; de Boer, R.J. Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk. *Sustainability* **2022**, *14*, 4937. <https://doi.org/10.3390/su14094937>

Academic Editor: Rui Cunha Marques

Received: 10 March 2022

Accepted: 11 April 2022

Published: 20 April 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Organizations need to adapt to changes and disruptions in their business environment as well as to address internal problems within their structures and operations, such as safety and security. To meet these challenges, organizations apply ISO management systems standards and strive to reach ISO certifications to prove that they have the mechanisms and control structures needed to manage their risk and be resilient in case of a hazard or threat.

ISO defines a standard as a “document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context” [1]. ISO has developed over 24,259 International Standards (<https://www.iso.org/standards-catalogue/browse-by-ics.html>, accessed on 9 March 2022). There are two types of ISO standards, the management system standards and the guidelines. There are many ISO management standards, and they address problems that cover a wide range of topics, e.g., ISO 9001 quality management [2], ISO/IEC 27001 information security [3], ISO 45001 occupational health and safety [4], ISO 22000 food safety [5], ISO 13485 medical devices [6], and ISO 37001 anti-bribery [7].

It is, however, a potential problem that organizations with ISO certification may feel safe and secure and still overlook or not pay attention to “hidden” risk. There is a need to create benchmarks for ISO standards to address this problem.

This article reports on the development of a risk-oriented benchmarking model based on risk science. It furthermore reports the findings when applied in a real-life case study conducted on six operating organizations, all of which are ISO certified and need to manage their business risk. Being ISO certified means that the organizations rely on ISO management system standards and guidelines, hereafter referred to as ISO standards, as tools for their risk management systems.

The authors' motivation for this study originates in decades of work experience in risk management, from the application of ISO standards in ISO certified organizations, and the auditing of ISO management systems. According to the authors' experience, the application of ISO standards and ISO certifications are no assurance of the efficacy of a risk management system. The risk terminology in ISO standards is not aligned with risk science and the ISO standards give limited guidance on how to analyze, assess, and manage risk [8]. Therefore, the aim of this study was twofold:

1. To develop a benchmarking model for risk management based on scientific literature and ISO standards in order to assess the efficacy of real risk management systems and see whether hidden risk can still be identified through ISO standard risk management systems and the risk assessment process used by operating organizations.
2. To test the benchmarking model on six real-life and ISO-certified risk management systems.

The organizations in this study are all certified by an accredited certification body [9] to at least one ISO management system standard [10], e.g., ISO/IEC 27001 [3], ISO 9001 [2], ISO 14001 [11], ISO 45001 [4], and ISO 13485 [6]. All these standards refer to ISO 31000 [12] as risk management guidelines. Managers of all six organizations were willing to participate in this case study because of increasing business need for analyzing and managing risk. They were interested in finding ways to evaluate the efficacy of their risk management systems in terms of finding hidden organizational risks through the risk assessment process used by the organizations, and to improve their risk analysis technique. Based on a previous study [8], it is hypothesized that certain risk issues will be evident in practice, provided a benchmarking tool (model) can be applied. Examples of such issues are the ability to capture risk in complex systems and that risk criteria can be unclear in ISO risk management systems.

The support and guidance given in ISO standards was investigated from a practical perspective. Testimonials and information provided was evaluated and confirmed through document review and meetings organized as external audits, in accordance with ISO 19011:2018&2011, Guidelines for auditing management systems [13]. The study lasted five years intermittently, from 2014 to 2019. In the meantime, some of the risk management systems evolved and therefore some records were updated, for example, results from risk assessments. Findings in this study take notice of risk management changes made by the organizations until the end of 2019.

The novelty of this study lies in the connection made between risk management systems in businesses and risk science. In addition, benchmarking theory is used to develop a benchmarking model, based on risk issues discussed in recent scientific articles that can be used to assess the efficacy of risk management systems in real ISO-certified organizations. The efficacy of such risk management systems can be difficult to measure because ISO standards are not based on risk science and provide little guidance on how to do so. Due to the growing importance of risk management in all business operations, management, and use of standards, it is important to find ways to measure the efficacy of risk management in a better way than hitherto.

In Section 2, the context for the study is described; in Section 3, the research methodology is illustrated; in Section 4, the results are presented; in Section 5, a discussion on the results is given; and in Section 6, conclusions are drawn.

2. Context for the Study

ISO standards were initially developed as quality standards where the users of the standards define their own quality criteria. Certification audits aim at verifying that the quality is as defined by an organization, whatever it may be. Now that risk management has become an important part of all ISO management systems standards (since 2015) [8,14], the question arises as to whether risk should be treated in a similar way. That is, if the willingness to take risk and the risk taken in ISO certified organizations is entirely the decision of the organizations' managers, and if not, how to evaluate the quality of the risk management. Quality is a unilateral decision of the organizations [15,16], but can risk be treated as a strategic variable like quality? The risk must be identified and understood to be able to assess it and decide if and how it should be treated. Here, the application of the standards varies regarding risk and quality, and, for example, auditors face a challenge when evaluating a risk management system. Managing risk and auditing risk management systems requires knowledge of risk management, often expert knowledge on risk analysis techniques on one hand and the subject facing risk on the other hand (e.g., design, development, production, services, operations). According to the authors' knowledge, no formal benchmarking models have been used until now as tools to evaluate the efficacy of ISO risk management systems.

Section 2.1 reviews recent developments influencing the development of benchmarking models regarding ISO standards. Section 2.2 reviews the risk management guidelines in ISO 31000, the structure, and use of the standard. Section 2.3 reviews selected scientific literature on risk issues in risk management systems, selection based on findings in recent article on risk management guidelines [8]. Section 3 describes the development of a benchmarking model used in this article for reviewing and evaluating the six real-life ISO risk management systems in this study.

2.1. Recent Developments Influencing the Development of Benchmarking Models

The Cambridge dictionary defines benchmarking as “the act of measuring the quality of something by comparing it with something else of an accepted standard” (<https://dictionary.cambridge.org/dictionary/english/benchmarking>, accessed on 9 March 2022). Benchmarking is therefore an important tool to help organizations to continuously improve the quality of their products and services. It is a popular tool in industry [17–20], but it is also used in the health service to improve patient outcome, for example in surgery [21]. In this study, the quality is limited to the efficacy of the risk management system. The Cambridge dictionary defines efficacy as “the ability [. . .] of a method of achieving something, to produce the intended result”. In this, section some examples of benchmarking contributions will be reviewed.

Herbst et al. [17] discuss benchmarking in cloud computing, which in recent years has become a significant part of information and communication technology. Benchmarks play an important role as evaluation tools during system design, development, and maintenance. They are therefore the basis for informed decisions. Herbst et al. lay a foundation for benchmarking cloud computing settings, one of which is operational risk. They use risk as a quality aspect reflecting the impact of running an application in cloud infrastructures and define operational risk as a group of metrics determining the risk of production systems running in cloud environments.

Kounev et al. [18] expand the discussion on benchmarking in information and communication technology in their book “Systems Benchmarking—for Scientists and Engineers” on the theory and practice of benchmarking. Due to the increasing importance of risk management, risk management benchmarking has now become an important research field. Kounev et al. discuss how benchmarks play an integral part in the evaluation and validation of new approaches and methodologies in research. The book focuses on the benchmarking of systems and components used as building blocks of modern information and communication technologies applications. In traditional benchmarking, the emphasis has been on evaluating performance, generally understood as useful work accomplished by

a system (or component) compared to the time and resources spent. Kounev et al. describe how performance benchmarks have contributed significantly to improve successive generations of systems. They describe how research on dependability benchmarking has increased beyond traditional performance benchmarking in the past two decades. They also note that resilience benchmarking faces challenges related to the integration of dependability, performance, and security benchmarking as well as to the adaptive characteristics of the systems under consideration.

Olawumi and Chan [19] present a study on the development of a benchmarking model for information modeling for buildings. This concerns “a repository of digital information which facilitates the efficient management of project information from conception by way of simplifying and presenting a real-world simulation of a pre-conceived project facility”. A qualitative approach was used to form the foundation of the proposed model. An assessment template and scoring system were developed to support the benchmarking model by providing a quantitative metric system for the proposed model. Olawumi and Chan conclude that construction organizations and project teams can benefit from the benchmark model and use the template and the associated scoring system to assess the level of information modeling innovation for buildings. They also conclude that their benchmarking model helps validate the implementation of the best practice framework in a project and improve the management of project information throughout the building lifecycle.

Van der Voordt and Jensen [20] compare the benchmarking theory and performance measurement with current practice and data from different work environments. To add value to an organization, workplaces must provide value for money by a positive trade-off between the benefits. They must support the organizational objectives and processes, with regard to the cost, time, and risk connected with achieving these benefits. They find that both quantitative and qualitative performance indicators, including hard and soft factors, are needed to define the trade-off between the costs and benefits of interventions in corporate real estate, facilities, and services, and to cope with the interests and needs of different stakeholders. Risk and risk expenses are amongst the value parameters they discuss.

Staiger et al. [21] address application and improvements in health care through benchmarking. They propose a systematic benchmarking approach in surgery, including the establishment of best achievable postoperative outcomes. According to Staiger et al., a standard approach for determining benchmarks enables self-assessment in surgical outcome and helps detect improvement opportunities. They emphasize that the intention of benchmarking in surgery is to stimulate surgeons’ genuine endeavor for perfection, rather than to criticize the surgeons’ performance or the health service. The goal must however be the improvement in patient outcome. They mention that new benchmarks should be defined in connection with high-risk groups, risk profiles, and risk adjustment.

Hartono et al. [22] discuss models for benchmarking qualitative data. In data envelopment analysis, performance evaluation is generally assumed to be based on a set of quantitative data. When evaluating processes or making decisions, it is, however, often necessary to take qualitative factors into account. They mention that some qualitative data measurement approaches have disadvantages when assessors provide judgment and cannot model the computational trust considering hesitancy, vagueness, and uncertainty. They propose a “hesitant fuzzy linguistic term sets” model which provides value for both input and output of decision maker units, based on a qualitative and sometimes hesitancy-based assessment. The results of Hartono’s and Abdullah’s study indicate that in data envelopment analysis the assessor can perform a good assessment in the form of qualitative data on the input and output of each decision maker units and then evaluation results will be available for use in the benchmarking process with the data envelopment analysis.

Mangla et al. [23] explore the relationship between various risk management strategies and practices in order to design and thus enact a suitable plan for supply chain risk mitigation. They discuss benchmarks for green supply chain managers and planners to help them model and assess risks and possible failures associated with their work. They use fuzzy failure mode and effects analysis approach to identify and assess the risks

associated with green supply chain. Mangla et al. conclude that their findings will help companies to reduce risk and its consequence, but also in enhancing its ecological-economic business sustainability.

Hoffmann et al. [24] study the antecedents of supply risk management performance. They use speed consortium benchmarking to explore the concepts of supply risk monitoring and mitigation. They identify not only the antecedents of supply risk management performance, but also the moderating effect of different supply risk management principles on the relation between uncertainty and supply risk management performance. Their study shows the relevance of developing general risk management structures and capabilities (i.e., risk management process maturity) to manage risk successfully. Their findings indicate that the implementation of a risk management process is even more important than the proper selection of individual risk monitoring and mitigation strategies.

Björklund [25] presents the development of a benchmark tool that can be applied to improve corporate social responsibility in purchasing. The tool was tested on two organizations which illustrates how the benchmarking tool can be applied. It provides a simple and systematic approach for evaluating a company's performance, improves transparency, and enhances cross-company comparison. The benchmark tool addresses both quantitative and qualitative aspects. Björklund concludes that it is of large importance to combine quantitative and qualitative measures in this area as quantification can be misleading if used in isolation.

Moriarty and Smallman [26] conduct a study on the theory of benchmarking. In their article, they review the epistemology of benchmarking and identify methodological elements of the theory of benchmarking. They discuss critiques of benchmarking which focus on three areas: (1) information (the reliability of exemplar information); (2) implementation (the intangibilities associated with implementing benchmarking); and (3) theory (the lack of a theoretical framework that distinguishes effective from ineffective efforts). This critique detracts from the potential advantages benchmarking appears to offer. The literature review they conduct shows overwhelmingly pragmatic approaches to benchmarking (that is, process-driven, case-oriented, and generic) as opposed to theoretical. Where theories are referred to, they center on the utility of benchmarking in terms of organizational learning and reasoning as well as economic enhancement.

MacGillivray et al. [27] describe the application of a capability model to benchmark the risk management maturity of eight water utilities in different countries. Their analysis codifies risk management practice and offers practical guidance on how utilities can more effectively use various risk analysis techniques for optimal, credible, and defensible decision making. Their case study shows that good risk analysis practices include: (a) use of initiation criteria for applying risk assessment techniques; (b) the implementation of formalized procedures to guide their application; (c) peer reviews; and (d) auditing. This ensures procedural compliance and provides quality assurance. MacGillivray et al. also identify common weaknesses, likely to be representative of the water utility sector they covered in their study, notably a need for improved risk knowledge management, education, and training in the discipline.

The examples of benchmarking contributions reviewed in this article describe various challenges, recent developments, and issues that are important for state-of-the-art benchmarking. The literature confirms the importance and challenges of benchmarking in the assurance of quality in risk management. The results can be summarized as follows:

1. Benchmarking is important for risk management [17,18,20,21,23,24,27].
2. Benchmarking is an important tool for performance evaluation and improvement processes of organizations [17–20,22,25,26].
3. In benchmarking, it may be necessary to combine quantitative and qualitative factors [17–20,22,25,26].
4. A scoring system helps in defining and verifying the “quality” of risk management actions [19,22,27].

5. A benchmarking system can be applied to stimulate a genuine endeavor for perfection, rather than to judge or criticize [21].

2.2. Risk Management in ISO Standards

ISO 31000 [12] is the main ISO guideline for risk management and according to ISO the standard “provides a common approach to managing any type of risk and is not industry or sector specific” (<https://www.iso.org/standard/65694.html>, accessed on 9 March 2022). It is intended for general guidance on risk management systems and not for certification. The first version of the standard was published in 2009 and this case study was originally based on that version. In an updated version, published in 2018, the principles of risk management have been reviewed. Greater emphasis is put on leadership by top management to ensure that risk management is integrated into all organizational activities, starting with the governance of the organization [28]. Greater emphasis is also put on the iterative nature of risk management, drawing on new experiences, knowledge, and analysis for the revision of process elements, actions, and controls at each stage of the process. According to the standard, risk management is based on the principles (described in clause 4), framework (described in clause 5), and process (described in clause 6). This is illustrated in Figure 1.

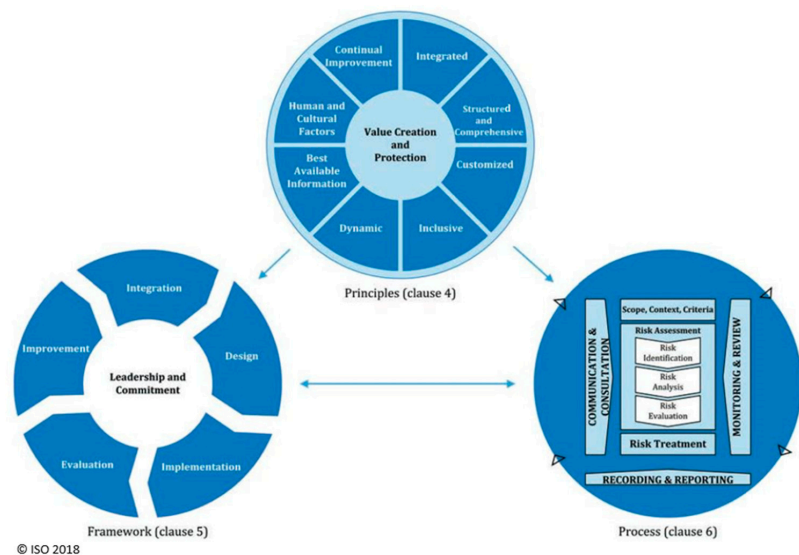


Figure 1. Graphical illustration of risk management from ISO 31000:2018 [12], principles, framework and process. Figure published with permission from Icelandic Standards.

The principles are the foundation for managing risk and should be considered when establishing the risk management framework and processes of an organization. The purpose of the risk management framework is to assist the organization in integrating risk management into activities and functions. The effectiveness of risk management depends on its integration into the governance of the organization, including decision making [29]. The components of the framework should be customized to the needs of the organization. Properly designed and implemented, the risk management framework will ensure that the risk management process is a part of all the organization’s activities, including decision making. The risk management process involves the systematic application of the policies, procedures, and practices to the activities of communication and consulting, defining the scope and establishing the context, assessing, and treating risk, monitoring, reviewing, recording, and reporting risk. Risk criteria should be aligned with the risk management framework and customized to the specific purpose and scope. It should reflect the orga-

nization's values, objectives, and resources, and should be consistent with policies and statements about risk management.

The ISO 31000 standard only contains guidelines, not requirements. The guidelines do not contain benchmarks for risk management in general, nor individual elements of the risk management principles, framework, or process. When auditing risk management systems that are based on ISO standards, the auditors apply the auditing standard ISO 19011 [13]. This standard is a general auditing standard, aimed at the auditing process itself and does not include benchmarks for risk management. The auditor is meant to seek written evidence (proof) of risk management, for example, the risk management process. The requirements are to be found in the ISO management system standard, such as ISO 9001 [2], ISO/IEC 27001 [3], ISO 45001 [4], ISO 13485 [6], and ISO 14001 [11].

In this study, the risk management process, as described in Figure 1, is used as a basis for benchmarking the risk management process in Section 3. The requirements regarding the risk management are obtained from ISO/IEC 27001, ISO 45001, and ISO 13485, and can be summarized as follows:

1. The scope of the risk management system must be defined.
2. The risk management process must be documented.
3. Policies regarding risk management must exist and be documented.
4. Internal audits must be conducted.
5. Management review and formal review and approval for suitability and adequacy, for example, review of operational planning and control, assessments of risk, nonconformity, and the efficacy of any corrective action taken.
6. Knowledge of all legal requirements must exist.
7. Risk and root cause analysis must be conducted.
8. Risk assessment/evaluation must be conducted.
9. Criteria must be set for the management system process and risk/quality acceptance.

When a requirement is required to be "documented" in an ISO standard, it is required to be established, implemented, and maintained. The requirements of ISO 9001 and ISO 14001 are less clear regarding risk management and it is not possible to build specific benchmarks on them [30].

2.3. Scientific Literature on Risk Issues in Risk Management Systems

Risk management systems, as described in ISO 31000, consist of risk management principles, framework, and process. According to ISO 31000, it is in the risk management process where the identification and evaluation of risk takes place, see Figure 1. The scientific basis of ISO risk management standards has been questioned in recent scientific literature [8,31–33]. ISO standards do not reference scientific literature, only other ISO standards and sometimes risk assessment techniques and handbooks. The only bibliographic reference in ISO 31000 is IEC 31010 [34]. IEC was first published in 2009 and then updated in 2019. It is a dual logo IEC/ISO standard for supporting ISO 31000. It provides guidance on the selection and application of systematic techniques for risk assessment. Some changes have been made regarding bibliographic references in the latest version of IEC 31010:2019. In version 2009, only 11 bibliographic references were made, all to other ISO/IEC standards. In the 2019 version, there are 91 bibliographic references. Many of them are not standards but handbooks and they are categorized in the bibliography according to risk techniques with no direct reference to risk science. Therefore, the aim of the literature review in this section is to identify risk issues that are the subject of scientific literature but not addressed in ISO standards. In this section, some examples of risk management science contributions are reviewed, as the basis for definition of benchmarks for a generic risk management process in Section 3.

Björnsdóttir et al. [8] conducted a review of 18 ISO standards (including ISO 31000, ISO/IEC 27001, ISO 45001, ISO 13485, ISO 9001, and ISO 14001) with regard to risk management to find out how well aligned the ISO standards are with scientific literature. Their study also aimed at evaluating if and how the standards address the management of risk

arising from complex interactions and emergent behavior that is inherent in present-day socio-technical systems. The study shows that ISO standards are not based on risk science and there are inconsistencies in both risk terminology and risk management guidelines. It also shows that it is difficult to standardize many risk-related factors, for example, the assessment criteria for something that is intangible. Björnsdóttir et al. show that ISO standards do not support users appropriately in analyzing and assessing risk when it comes to the complexity of socio-technical systems, emergent behavior, and non-linear causal relations.

Aven and Zio [31] analyze the foundational issues of risk assessment and management in their article. They discuss the needs, obstacles, and challenges for the establishment of a renewed, strong scientific foundation, suited for the current and future technological challenges. Among the issues Aven and Zio identify is terminology and fundamental principles; the risk management field lacks universally understood and well-defined terms. They also point out that risk analysis of critical infrastructure systems, e.g., power grids, is both challenging and important. Such systems are often complex and interdependent where system components interact on multiple scales of space and time. The system components are often heterogeneous and form a hierarchy of subsystems. There is a need for appropriate tools and techniques for analyzing risk and vulnerabilities in such complex systems. Furthermore, they mention issues regarding the scope and science of risk assessment and point out that quantitative risk assessment methods need to cover knowledge (description and characteristics) of the uncertainties.

Klinke and Renn [32] discuss a new approach to risk evaluation and management. They propose a new classification of risk types and management strategies for dealing with the problems of complexity, uncertainty, and ambiguity—with scientific accuracy, a reflection of social diversity, and political feasibility. This includes criteria for evaluating risk and a classification of risk types and risk management strategies. Their concept of risk evaluation criteria, risk classes, a decision tree, and management categories was developed to improve the effectiveness, efficiency, and political feasibility of risk management procedures. The main task of risk evaluation and management is to develop adequate tools for dealing with the problems of complexity, uncertainty, and ambiguity.

Cox [33] discusses the uncertainty involved in the use of risk matrices, which is a widespread way of assessing risk. The meaning of a risk matrix may be far from transparent, despite its simple appearance. Cox examines some mathematical properties of risk matrices and shows that they have the following limitations: (a) poor resolution; (b) errors; (c) sub-optimal resource allocation; and (d) ambiguous inputs and outputs. He demonstrates that, in general, quantitative and semiquantitative risk matrices have limited ability to correctly reproduce the risk ratings implied by quantitative models, especially if risk components such as frequency and severity are negatively correlated. Cox suggests caution in using risk matrices because they do not necessarily support good risk management decisions.

Aven [35] also addresses the weaknesses of risk matrices. They are a common practice for the characterization of risk, reflecting threats and their consequences and probability, as well as concepts such as risk factors and sources. His conclusion is that risk matrices in the traditional two-dimensional consequences-probability form should not be used. Such matrices need an additional knowledge dimension to capture and include the strength of knowledge judgements and rankings of risk factors and assumptions supporting the analysis.

Fellows and Liu [36] discuss boundary issues across multiple interfaces in engineering construction projects. Such projects have many boundaries between various stakeholders. According to Fellows and Liu, organizations engaged in such projects require permeable boundaries to allow information flow, knowledge sharing, and learning so that they can respond appropriately and quickly to changes. Thus, while formal boundaries may be fixed and rigid, informal boundaries in projects may need to be flexible and facilitate organizational adaptations for performance of constituent project activities, especially in project governance. The main concern here is to nurture cooperation, collaboration,

and commitment with respect to the diverse natures and interests of the participants. Complexity issues also arise through increasingly complex projects and their organizational structures. A high degree of specialization often needs the involvement of numerous specialized companies, each of which has its own boundary. The performance and success depend on how well the boundary activities are planned and managed. Fellows and Liu conclude that engineering construction projects are nested hierarchies of complex adaptive systems involving numerous, diverse stakeholders. Thus, performance requirements and parameters are emergent. The systems co-evolve, and any equilibria are dynamic.

Mikes [37] discusses boundary issues and work in risk management. Her field study in the banking sector suggests that the boundary work of risk experts advances two different approaches to risk management, depending on their calculative cultures. The financial crisis of 2007–2009 proved to be a challenge to risk management in the banking systems. Since then, the risk experts have tried to find ways to improve risk management. On one hand, there is a culture of quantitative enthusiasm, where risk functions are dedicated to risk measurement. On the other hand, there is a culture of quantitative skepticism, focusing on envisioning risk and aiming to provide top management with alternative future scenarios and with expert opinions on emerging risk issues. The study shows that those displaying quantitative enthusiasm strived to capture the complexity of risk decisions. As much judgment as possible is included upfront in the model design, so that the output of the model could be regarded as a close proxy to the underlying risk profile. Again, senior risk managers with a strong quantitative skepticism expanded the boundaries of the risk universe (all risk that could affect an entity) beyond modeling by creating fora for the envisioning of non-calculable risk objects. They relied less on formal models than on their own cognitive mental models, imagining alternative futures about which the existing models had nothing to say. They sought to anticipate emerging risk and uncertainties that are not measurable in order to guide discretionary strategic decisions, for which they were ready to take responsibility. Mikes discusses that “if risk officers are to uphold the ideal of measurement, they can only extend their remit to risks that can be described by a priori known or statistically knowable distributions. Alternatively, if they are to discuss and influence the management of non-quantifiable risks, threats, and opportunities (Knightian uncertainties), they have to venture outside the measurement framework”. She concludes that as risk management practitioners move forward in their work, theoretical and empirical researchers will be summoned to account for new realms, new definitions, and new purposes of risk management.

Zerjav [38] addresses the problem of boundary dynamics and issues of resources allocation in infrastructure projects. Due to their complexity and high social impact, such projects often face challenges in managing the design decision-making processes across disparate disciplinary and knowledge domain boundaries. Zerjav identifies the key role of resource allocation constraints, path dependency of project decisions, and problem-solving nature of design. He introduces the notion of design boundary dynamics for describing diverse cross-boundary coordination phenomena associated with organizing the design of infrastructure projects.

Lathrop and Ezell [39] address the validation of risk analysis. They describe, with a systems approach, that validation of a risk analysis should be based on how well the risk analysis supports risk management. When assessing how well the risk analysis supports risk management, it should be considered how well it supports the decision-making process. They conclude that the implementation of risk management actions results in what matters: the final consequences and residual risk.

The risk issues addressed in the literature can be summarized as follows and applied as benchmarks as presented in Section 3:

1. Scope and outer boundaries of a risk management system [31,36–38].
2. Interfaces (internal boundaries, departments, unclear responsibility) within a risk management system [31,36–38].

3. Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a risk management system [31,36].
4. Resources available to support a risk management system [33,38].
5. Risk analysis ability to capture complex systems and business operations [8,31,32,36–38].
6. Risk assessment ability to capture risk evaluation, e.g., with risk matrices [8,32].
7. Risk criteria setting in risk assessment [8,32].
8. Treatment of residual risk [39].

3. Development of a Benchmarking Model for an ISO Risk Management System

The benchmarking model developed and applied in this research is based on the literature review and context of the study as described in Section 2. It is divided into the following two steps:

Step 1: Validation and evaluation of the foundational elements of a generic risk management system that is based on ISO standards. Assessment template with a simple scoring system.

Step 2: Validation and evaluation of some of the most critical elements of the risk management process, according to ISO and scientific literature on risk management issues.

3.1. Step 1

An assessment template with simple scoring system can be used to evaluate the existence of the basic elements of a risk management system. Based on the findings in Sections 2.2 and 2.3, the following benchmarks were defined. The scoring system provides a quantitative metric system with simple scores such as “yes”, “no”, “not applicable”, and “not specified”. The proposed benchmarks are as follows:

1. Scope, context, and boundaries of the risk management system.
2. Compliance with regulative requirements concerning the business.
3. Certifications.
4. Policies regarding risk are documented.
5. Risk management system is documented.
6. Risk analysis is conducted in a formal way.
7. Risk assessment is conducted in a formal way.
8. Risk (acceptance) criteria are set.
9. Residual risk is addressed (identified and assessed).

3.2. Step 2

If a risk management system meets the criteria in Step 1 and the benchmarks are positive, the next step is to assess the quality in terms of efficacy of individual elements of the risk management system. In this study, the most important elements of the risk management process were put in focus and findings in Section 2.3 used as basis for benchmarks.

To assess the scope further, context, compliance, and conformity of the risk management system (no. 1–5 in Step 1), the following benchmarks were defined:

1. Scope and outer boundaries of the risk management system.
2. Internal boundaries and interfaces, complexity of the organizational structure, and distribution of accountability.
3. Hierarchical structure with regard to risk, both safety and security risk.
4. Resources, knowledge, and experience needed to support the risk management system.

Additionally, the following benchmarks were defined to further assess the efficacy of some of the most important elements of the risk management process (no. 6–9 in Step 1):

5. Risk analysis ability to capture complexity of the business operation and systems (foundation, method, technique).
6. Risk assessment ability to capture risk evaluation (ability to capture risk knowledge).
7. Risk criteria setting in risk assessment.

8. Identification and treatment of residual risk, risk that is left after formal risk mitigation/treatment.

Table 1 gives an overview of the benchmarks in Step 2. The first column shows the benchmark number, second column shows the benchmark name, third column shows the corresponding principle/framework/process in ISO 31000 as described in Section 2.2.

Table 1. Benchmarks with correspondence to ISO 31000:2018 [12].

No.	Benchmark Name	Corresponding Risk Management (RM) Principle/Framework/Process Clause in ISO 31000
1	Scope and outer boundaries of a RM system	Process (clause 6): Scope, context, and criteria (6.3)
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Process (clause 6): Scope, context, and criteria (6.3)
3	Hierarchical issues (layer issues, unclear hierarchical safety and security structure) within a RM system	Principles (clause 4): Structured, comprehensive, and dynamic RM Framework (clause 5): Leadership and commitment (clause 5.2) Process (clause 6): Risk assessment (clause 6.4) and risk treatment (clause 6.5)
4	Resources available to support the RM system	Framework (clause 5): Leadership and commitment (clause 5.2)
5	Risk analysis ability (foundation, method) to capture complexity	Process (clause 6): Risk assessment (clause 6.4)
6	Risk assessment ability to capture risk evaluation	Process (clause 6): Risk assessment (clause 6.4)
7	Risk criteria setting in risk assessment	Process (clause 6): Risk assessment (clause 6.4) and risk treatment (clause 6.5)
8	Treatment of residual risk, risk that is left after risk mitigation	Principles (clause 4): Continual improvements Framework (clause 5): Improvement (clause 5.7) Process (clause 6): Risk assessment (clause 6.4), risk treatment (clause 6.5), monitoring and review (clause 6.6)

4. Research Methodology and Hypotheses

After developing the benchmarking model described in Section 3, this research proceeded in the following five steps: (1) setting selection criteria for participants in the study; (2) selection of business sectors and organizations; (3) conducting of a risk management questionnaire based on the benchmarking model in Step 1; (4) follow-up interviews; (5) evaluation of the risk management process applying the benchmark model developed in Step 2. Figure 2 gives an overview of the research process. It describes the research methodology and its individual steps, also reflecting the structure of this article. The next two subsections describe the research methodology (Section 4.1) and the hypotheses put forward (Section 4.2).

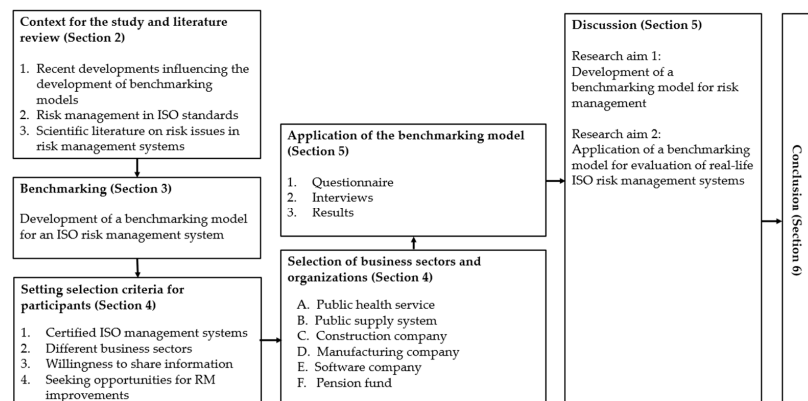


Figure 2. Research overview.

4.1. Research Methodology

4.1.1. Setting Selection Criteria for Participants in the Study

A desk study was conducted to define selection criteria and identify possible candidates for the research. Eligibility criteria were specified. The organizations should: (a) have a certified ISO management system, or at least be in the implementing phase of an ISO management system; (b) be from different business sectors; (c) be willing to share information from what were considered to be successful business operations or projects; (d) be seeking opportunities to improve their risk management process in general.

Organizations operating in six industry sectors were selected: (A) public health service; (B) public supply system; (C) construction company; (D) manufacturing company; (E) software company; and (F) pension fund. Table 2 shows a list of the organizations selected for this case study. The first column shows the organizations' type of business. The second column shows the business operations examined in this study. The third column shows the ISO standards each organization is certified to.

Table 2. Organizations examined in this study.

ID	Organization	Business Operation	Accredited ISO Certifications
A	Public health service	Processing of biological samples	ISO 9001
B	Public supply system	Operation of an electricity transmission system	ISO 9001, ISO 14001, ISO 45001
C	Construction company	Construction of an infrastructure facility	ISO 9001, ISO 14001, ISO/IEC 27001, ISO 45001
D	Manufacturing company	Manufacturing of a medical device	ISO 14001, ISO 13485
E	Software company	Software development	ISO/IEC 27001
F	Pension fund	Financial investments	ISO 9001, ISO/IEC 27001

All six organizations fulfil the research criteria mentioned above. Five of them already had accredited certification to one or more ISO standards when the case study started in 2014, one was in the implementing phase and received accredited certification during the time of the study, end of 2018. Written contracts were made with all organizations to ensure information security according to the requirements of ISO/IEC 27001:2013 [3] throughout and after the case study process. A contact person was nominated in every organization, responsible for the delivery of information, orally and written. After signing contracts and confidentiality agreements, meetings were held with the contact persons and their teams to inform them, explain the aim of the research, answer questions, and clarify expectations on both sides.

4.1.2. Questionnaire

The questionnaire (see Table 3) is based on the research framework described in Section 3. It was sent to the contact persons in each organization. Answers from questionnaires along with supporting documents (e.g., organizational manuals, description of processes and procedures, policy documents, and results from risk assessments) were received from all organizations. These data were reviewed with regard to benchmarks, content of information, and alignment with guidelines in ISO 31000.

Table 3. Questionnaire summary.

No.	Question/Topic	A—Public Health Service	B—Public Supply System	C—Construction Company	D—Manufacturing Company	E—Software Company	F—Pension Fund
1	General information						
1.1	Listed (on Nasdaq)	no	no	no	yes	yes	no
1.2	Number of employees (European Union classification)	51–250	51–250	251–500	501–5000	11–50	11–50
1.3	Number of local sites/offices	4	2	7	1	1	1
1.4	Number of countries with subsidiaries	1	1	1	18	2	1
1.5	Intl. business operations and export	no	no	yes	yes	yes	yes
2	Compliance						
2.1	Relevant laws and regulations for business identified	yes	yes	yes	yes	yes	yes
3	Certification						
3.1	Operations ISO certified	all	all	all	partly	all	all
3.1.1	... if yes, by an accredited certification body	yes	yes	yes	yes	yes	yes
3.1.2	... if yes, name of certification body	list	list	list	list	list	list
3.2	Non-ISO certifications	yes	no	yes	yes	no	no
3.2.1	... if yes, which parts	list	list	list	list	list	list
3.2.2	... if yes, which accredited certification body	list	list	list	list	list	list
4	Policies						
4.1	Safety and/or security policy exist	yes	yes	yes	yes	yes	yes
4.2	Documented safety and/or security policy exists	no	yes	yes	yes	yes	yes
4.3	Ref. to relevant law(s)/regulation(s) in policy documents	list	list	list	list	list	list
4.4	Other policy documents relevant to safety/security	yes	yes	yes	yes	yes	yes
5	Risk management system						
5.1	Formal risk management process in place	yes	yes	yes	yes	yes	yes
5.2	Risk assessment conducted	yes	yes	yes	yes	yes	yes
5.3	Risk analysis conducted	yes	yes	yes	yes	yes	yes
5.4	Internal control	yes	yes	yes	yes	yes	yes
5.5	Audits, internal and/or external	yes	yes	yes	yes	yes	yes
5.6	Review process	yes	yes	yes	no	yes	yes
6	Risk analysis						
6.1	Formal methodology used	yes	yes	yes	yes	yes	yes
6.2	Use of special software solution for risk analysis	no	yes	no	no	yes	no
6.3	ISO guidelines used for doing risk analysis	no	yes	yes	yes	yes	yes
6.4	Likelihood of risk assessed	no	yes	yes	yes	yes	yes
6.5	Risk evaluated	yes	yes	yes	yes	yes	yes
7	Risk assessment						
7.1	Tangible assets registered	yes	yes	yes	n.a.	yes	yes
7.2	Intangible assets registered	yes	yes	yes	n.a.	yes	yes
7.3	Threats identified	yes	yes	yes	n.a.	yes	yes
7.4	Consequence of risk assessed	yes	yes	yes	yes	yes	yes
7.5	Risk calculated	no	yes	yes	yes	yes	yes
7.6	Systematic risk mitigation with controls	yes	yes	yes	yes	yes	yes
7.7	Risk calculation after selecting controls—efficacy of controls assessed	no	yes	n.s.	no	yes	yes
7.8	Assessment on efficacy and usefulness of risk analysis in terms of cost	no	yes	yes	no	no	no
7.9	Risk information used for improvements—someone responsible	yes	yes	yes	yes	yes	yes
7.10	Result of risk assessment documented	yes	yes	yes	yes	yes	yes
7.11	Result of risk assessment used to learn from it	n.s.	yes	yes	yes	yes	yes
8	Risk criteria						
8.1	Risk criteria set	no	yes	yes	yes	yes	yes
9	Residual risk						
9.1	Residual risk assessed	no	yes	no	yes	yes	yes

“list” = list provided; “n.a.” = not applicable; “n.s.” = not specified.

4.1.3. Interviews

After collection, review, and analysis of data from the questionnaire, follow-up meetings were organized and held as audit meetings according to ISO 19011 [13]. The aim was to confirm the information given in the questionnaire. This was done by obtaining evidence, review, and confirming data integrity and compliance with records received. Records on incidents and nonconformities were reviewed and the efficacy of the ISO plan-do-check-act cycle was examined with regard to corrective actions. Meetings were recorded where permission for recording was obtained. The follow-up meetings led to a variety of findings. Subsequently, more information and evidence were gathered, and testimonies recorded. The case study lasted five years intermittently. In the meantime, some of the organizations developed their risk management systems and therefore some records (e.g., results from risk assessments) were updated.

4.2. Hypothesis

Since all participants in this real-life study are certified to ISO management system standards that require risk management, it can be expected that all major aspects of risk management are present and for the most part well documented. However, ISO standards lack guidance on risk management as demonstrated by Björnsdóttir et al. in a previous study [8]. Consequently, it is expected that risk management, and particularly the analysis of risk, is executed in an unsatisfactory manner. Assuming that the representatives of the organizations in this study are describing the true situation in their organizations, it is therefore hypothesized that certain flaws in risk management will be evident in practice. The benchmarks developed, based on the literature review conducted in Section 2.3 and presented in Table 1, are used to evaluate the risk management systems examined in this study.

5. Results

The results of this study are presented in the following six subsections, one section for each organization. The results are presented in tables and discussed, and conclusions drawn. An overview of the results from the questionnaire is presented in Table 3. The topics/questions are grouped into categories, intended to:

1. Capture general information regarding the business operations and the risk management system: scope, interface, organizational structure (hierarchy and layers), and resource issues. This is consistent with topics no. 1–4 in Table 3 and benchmarks no. 1–4 in Table 2.
2. Capture more specific information about the risk management system: foundational issues, risk analysis technique, ability to capture complex risk, ability to evaluate risk, including residual risk. This is consistent with topics no. 5–9 in Table 3 and benchmarks no. 5–9 in Table 2.

The first two columns show the number and name of question/topic in the questionnaire. The following six columns show the results for individual organizations. The results are examined and explained in the next six subsections, one subsection for every organization. In most cases, the answers are “yes” or “no”. The answer “list” means that a list was provided, “n.a.” means not applicable, and “n.s.” means not specified.

5.1. Public Health Service

The public health service (organization A in Table 2) is an independent part of a university hospital. It is responsible for the processing of biological samples, e.g., blood. The main operations are in the hospital area, but it also has two sites outside the main hospital area and a mobile sample collection unit. The service of the organization includes collecting and processing of blood, testing, education, services regarding cells and tissues, transplantation, and stem cell therapy. Part of the infrastructure, e.g., information technology support and technical assistance, is in the hospital’s organizational chart under a different management system. During the time of this study, the contact person moved on from being a quality

manager to becoming head of department. The risk management system developed in such a way that risk analysis has become a part of all working procedures, which was not the case at the beginning of the study.

5.1.1. Results from the Questionnaire

The public health service is certified to ISO 9001 [2] to ensure the correct working procedures, quality, and safety of the products and services. It also has other types of specific certifications and operating licenses not related to ISO. The quality policy is documented and addresses both safety and security, but no other ISO management system policy documents exist. There is good knowledge of the legal environment. A formal risk management process is in place, as a part of the ISO management system. This means that risk assessment and risk analysis are conducted, there is internal control, regular audits (internal and external), and a management review process. A formal risk analysis technique is used in the form of a two-dimensional risk matrix in Excel. ISO risk management guidelines are not used, both tangible and intangible assets are identified, and risk is related to assets. Threats to assets are identified, and consequence of risk assessed. Likelihood of risk is not a factor in the assessment, risk is not calculated, risk criteria are not set, and residual risk is not assessed.

5.1.2. Results from the Interview

The head of department (former quality manager) of the public health service was interviewed. The interview revealed that risk management of the organization is mainly based on international health science norms and standards published by the European Commission and the World Health Organization, and not on ISO standards. One of these guidelines is the Guide to the Preparation, Use, and Quality Assurance of Blood Components [40]. The World Health Organization, WHO, has also published international health science norms and standards, e.g., the WHO Action Framework to Advance Universal Access to Quality and Safe Blood and Blood Components for Transfusion and Plasma Derived Medicinal Products [41]. These publications define hazards within the health service environment. For example, the most hazardous states regarding blood processing involves blood leaving the organization with one or more of the following hazards: (a) blood is mislabeled; (b) contaminated blood passes screen; (c) blood spoils within the organization.

Risk analysis is conducted on many levels and is not based on ISO 9001, since there is no guidance on risk analysis in the standard, and only partly based on ISO 31000. In case of blood donation, the risk analysis starts when a blood donor comes to the organization. A healthcare professional interviews the donor and assesses his or her suitability for donation. The assessment is documented. Another part of the risk assessment is the quality control process of blood components, based on content and sample requirements. The quality control is done by trained healthcare professionals, records are made in Excel sheets and in a database. Risk assessment is also done as a part of an incident registration process, which includes a review and evaluation of an incident. However, work is not always done according to that process. A two-dimensional risk matrix is used to assess an incident and determine a risk factor, based on impact of risk and likelihood of recurrence, both on a scale of 1 to 5. Three different colors (green, yellow, red) are used to show the severity of a risk factor. The risk analysis became more formal after this study started and at the end of it, more employees had been mobilized to take part. There are risk issues regarding, e.g., information technology support and assistance, which is not a part of the risk management system of the organization but a part of the hospital's central infrastructure.

The interview also revealed that there are risk factors that have not been registered or formally assessed. The department head is aware of these risk factors but has not found a way to either assess them or treat them because they are on the border of the business scope. This risk is related to the delivery and use of blood products and cooperation with health organizations receiving blood products, but not having a formal quality or risk management

system themselves. There are also risk issues in interactions and communications with health authorities that has neither been registered nor treated.

5.1.3. Summarized Results from the Public Health Service

The public health service is an important part of the infrastructure of the health system. It is not a competitive business entity, but the ISO certification shows ambition in operation and good service. The procedure for risk analysis is not yet fully documented. It is difficult to manage risk on the border of the business scope and risk related to communication. Lack of communication with external parties has been difficult to capture. It has also been difficult to communicate risk information to authorities. Table 4 presents a summary of the results from the public health service.

Table 4. Results from the public health service.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	Outer boundaries of RM system stretched into other health care institutions without compliance with ISO procedures	True
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Boundary issues regarding joint service and infrastructure of the hospital	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Two-dimensional risk metrics does not capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk criteria unclear	True
8	Treatment of residual risk	Residual risk not addressed	True

5.2. Public Supply System

The public supply system (organization B in Table 2) transmits electricity from generation stations to regional electricity distribution operators and power intensive users by way of a high voltage transmission system (power grid). The operation is regulated by the national energy authority which determines the revenue cap on which the electricity tariff is based. The public supply system is a critical infrastructure system and care must be taken when transmitting the electricity through the system to maintain the balance between consumption and production of electricity.

5.2.1. Results from the Questionnaire

The system operator has one business site other than the main office and is certified to ISO 9001 [2], ISO 14001 [11], and ISO 45001 [4] (previously OHSAS 18001). ISO/IEC 27001 [3] is in implementation phase. Written ISO management system policy documents exist where safety, security, and environmental risk is addressed. There is good knowledge of the legal environment. A formal risk management process is in place as a part of the ISO management system. This means that risk analysis and risk assessment are conducted. There is internal control, regular audits (internal and external), and a management review process. A formal risk analysis technique is used, implemented in a risk assessment software solution. ISO risk management guidelines are used. Both tangible and intangible assets are identified, and risk is related to assets. Threats to assets are identified and consequence of risk is assessed. Likelihood of risk is a factor in the assessment and risk is calculated. Risk management includes continuous improvements, systematic risk mitigation, assessment of risk control efficacy, cost analysis, documentation, and risk learning process. Risk criteria are set but residual risk is not assessed.

5.2.2. Results from the Interview

The head of system operation was interviewed. The interview revealed that the risk assessment process and risk analysis technique are mainly based on ISO/IEC 27001, which has not yet been fully implemented. Risk is analyzed and assessed in Excel templates and results from risk assessment, then stored in a central SQL database. Risk factors are identified, registered, and categorized in main categories and subcategories. Description of each risk factor, cause, and effect are registered. Likelihood and impact are estimated in numbers and then risk is calculated as a multiple of likelihood and impact, $\text{risk} = (\text{likelihood of risk}) \times (\text{impact of risk})$. Both likelihood and impact are integers on a scale of 1–4. Risk tables in Excel and two-dimensional matrices with four different colors are used to show the severity of each risk factor. For each risk factor, there is one responsible person. Responsible departments are also registered, there can be more than one. A short description of an action plan to mitigate risk is registered with a follow-up plan, which is sometimes left unfilled. In some cases, if related to the finance department, a policy document is referenced with a note of measurements and risk criteria. A bottom-up risk assessment technique is used, and each department is responsible for assessing its own risk. All risk assessments are then collected into one risk library. Risk assessments are also conducted as part of project management. A risk overview with summary and statistics is provided through a management software interface.

Results from risk assessment and incidents that have happened reveal weaknesses in the system. To mitigate this risk, some parts of the system (old overhead lines) need to be renewed and some new lines must also be built in areas that are considered natural reserves. There have been disputes over how to build and maintain the system, which concern the choice of laying high voltage overhead lines and/or underground cables. Disputes with landowners who either do not want a power line across their land or want unacceptable compensation for their land cause delay. Further enquiry revealed that some existing risk factors have neither been registered nor assessed because it is not clear who is responsible. This applies to risk caused by hybrid threats and threats such as pandemics. Risks related to the lack of public policy support, international politics, and trends in technology (e.g., smart grid) that could affect the electricity transmission systems have not been identified.

5.2.3. Summarized Results from the Public Supply System

The public supply system is a critical infrastructure system. Risk analysis has revealed that electrical power security is insufficient in some places and breakdowns have led to power outages. The bottom-up risk analysis method has led to causal relationships between risk factors not being identified, the root cause has not been identified, and risk that does not clearly fall within one of the departments is not identified. Table 5 presents a summary of the results from the public supply system.

Table 5. Results from the public supply system.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	Risk associated with stakeholders not always addressed	True
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Internal boundaries well defined but bottom-up risk assessment within departments has led to causality between risk factors not being identified	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	Hierarchical issues found	True
4	Resources available to support the RM system	Resource issues found	True
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Two-dimensional risk metrics does not capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk criteria sometimes unclear	True
8	Treatment of residual risk	Not every known risk is included in the risk assessment and treated therefore left as residual risk	True

5.3. Construction Company

The construction company (organization C in Table 2) constructs infrastructure facilities/products, operates them, and sells the product. The construction of each facility/project involves complex systems and equipment, as well as challenging construction work in often extreme conditions. The project analyzed in this study was divided into several contracts, some regarding construction work, some for equipment, and others for systems. The construction phase of the project analyzed in this study took five years and was finished in 2014. Altogether, the project took ten years including the preparation phase.

5.3.1. Results from the Questionnaire

The construction company has seven offices and is certified to ISO 9001 [2], ISO 14001 [11], ISO/IEC 27001 [3], and ISO 45001 [4]. Written ISO management system policy documents exist where risk regarding safety, security, and environment is addressed. There is good knowledge of the company's legal environment. A formal risk management process is in place as a part of the ISO management system. Risk analysis and risk assessment are conducted. There is internal control, regular internal and external audits, and a management review process. A formal risk analysis technique is used and implemented in Excel templates. ISO risk management guidelines are not used during the construction phase. Risk is assessed regarding threats/hazards, likelihood, and consequence. Risk management includes continuous improvements, systematic risk mitigation, cost analysis, documentation, and risk learning process. Efficacy of risk controls is not assessed. Risk criteria are partly set, and residual risk is not assessed in a formal way. Results from risk assessments are documented and used to learn from them.

5.3.2. Results from the Interview

The interview with the project risk manager revealed that the construction company takes a holistic approach to risk management and the company's risk manager is responsible for coordinating overall risk management tasks and maintaining ISO certifications. However, risk management in individual projects is led by a project risk manager. Both the risk manager of the construction project and the company risk manager were therefore interviewed. Two risk management teams were formed in the project, one in the preparation phase and another in the construction phase. In the preparation phase, a risk consultant led the work together with the project manager. The risk work in the construction phase was led by the project risk manager who worked closely with the project management team throughout the construction phase. Both teams included experts from the company and external consultants. Regular meetings were held, risk associated with the project identified, and actions taken to reduce the risk. The project risk manager kept records of all risk-related information during the project time. When the project was finished, a final report was compiled on project health, safety, and environmental issues where risk assessment and risk management were included. Despite complications during the project time, the project was considered an overall success. There were three measurable reasons for this: (a) the project time was met; (b) the cost estimate was met; (c) there were no serious injuries.

Although much energy and time was spent on the risk analysis, the project risk manager acknowledged that risk assessment is an underestimated part of work in projects like this one. Risk analysis is the basis for disciplined working procedures, to ensure that the right decisions are made at the right time, and to avoid mistakes. Often, the environmental impact is controversial and different interests need to be balanced. Stakeholders' views were included in the risk analysis. Contractors had to submit their own risk assessment for every work item before they could start the work. Risk factors were reviewed in risk meetings and compared with company own assessment. This way, both parties (construction company and contractor) could assess risk factors together. One reason for this is that the construction company (buyer) did not always know what equipment the contractor would be using. The aim of the meetings was to achieve the widest possible knowledge and understanding

of all risk related to the project. The meetings were sometimes big and difficult to manage, like brainstorming sessions. Discussions tended to drift, and much discipline was required. People got ideas and started discussing solutions while analyzing risk. This made the risk analysis difficult and complicated in practice. The goal was to somehow measure the outcome, results, and efficacy of the risk analysis, but no good way was found for such measurements. The ISO risk management guidelines were not used. The project risk manager considers the need for effective risk analysis methods in big construction projects both urgent and growing. The risk analysis of projects such as this one is often centered on operational risk in terms of finance. In the opinion of the project risk manager, simple risk models are good to get started and lay out the risk analysis. Then, it is necessary to dive deeper into different parts of the risk model. It can be disadvantageous for the construction company to tie things regarding construction projects too much with standards and regulation requirements. It can lead to overdesign and associated unnecessary costs.

The company's risk manager stated that there is one uniform risk assessment process within the whole company. He is responsible for the company risk register stored in a Microsoft SharePoint system. Other employees are responsible for assessing risk in Excel spreadsheets. The risk analysis is defined as identification of risk, registration, categorization, scoring, and comparison with risk criteria that are set in the beginning. This includes considering the business goals of the company, goals of risk management, and goals of every project. Scope and goal setting may differ. A matrix with colors and two scales, EBITDA, and company image is used to assess high-level company risk. Different scores are used for analyzing risk at other levels in the company. Moreover, the risk criteria differ depending on what is relevant to different departments and projects. The purpose of risk analysis is to: (a) ensure that the company achieves its goals; (b) provide an overview of risk; (c) ensure that the company does not suffer major setback/incidents that can have significant negative impact on its operations. In risk analysis, all risk factors are considered, regardless of likelihood and impact, but there needs to be a clear incentive and expectation of benefits before starting a risk analysis. Risk analysis is time consuming and often complicated. It is important that risk experts can communicate the risk information and make it easy for others to understand. The company risk manager believes that although the risk framework may be different within organizations, the technique/method and process of risk analysis can still be the same. Communication, information sharing, solutions, monitoring, and feedback may all be different.

In the opinion of the company's risk manager, risk analysis is too seldom a part of decision making. His view is that risk analysis must be built into company culture. It should be as natural to analyze risk as to calculate expected return on investment. This is often not the case; people tend to spend too little time on risk analysis when making decisions and simply assume they know everything there is to know. It is difficult to estimate the value of risk analysis and it can be challenging to explain and get people involved. It seems easier to analyze and assess risk where quantitative measurements are made, but qualitative evaluation is often necessary to reach full understanding. For many, it turns out to be difficult to choose a risk score or put a number on the risk. To be able to develop a risk culture within a company, it is important to review completed projects to learn from the experience, to give and get feedback, to improve and optimize the risk analysis process. If risk analysis is continuously applied as a business tool in daily use, it can aid in finding opportunities to improve the business. His opinion is that ISO standards can be helpful together with management system tools once risk has been identified. ISO 31000 [10] provides support and IEC 31010 [34] points out various techniques to analyze risk. The challenge, however, remains to identify the hazards, threats, and risk.

5.3.3. Summarized Results from the Construction Company

In this study, a single but complex construction project, lasting five years, was analyzed. Other parts of the organizations were not analyzed. Many contractors took part in the project. The company has been ISO certified to four management system standards

for decades and its risk management system is mature. Through many comprehensive construction projects, the company has developed a strong risk management culture. This has led to the company's risk management leaders being aware of the importance of risk analysis and risk management. Both the project risk manager and the company's risk manager believe that there are still opportunities to improve risk analysis and risk management within their company, e.g., with better coordination and integration into the company's overall management. Employees could be better educated and given better guidance in their work. ISO standards in general provide good support for risk management. The problematic question is: How much is a company willing to invest in the implementation and improvements of a risk management system? Key risk indicators need to be defined for indication of imminent risk. It is challenging to define what should be measured and monitored and it needs to be carefully done. Table 6 summarizes the results from the construction project. No issues were reported for benchmarks no. 5, 6, 7, and 8 in Table 6. This means that the hypothesis could not be verified.

Table 6. Results from the construction company.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	No issues reported	Not verified
6	Risk assessment ability to capture risk evaluation	No issues reported	Not verified
7	Risk criteria setting in risk assessment	No issues reported	Not verified
8	Treatment of residual risk	No issues reported	Not verified

5.4. Manufacturing Company

The manufacturing company (organization D in Table 2) develops, produces, and sells medical devices. The subject in this study is a microcomputer-controlled (bionic) device. The questionnaire was answered by a project manager with help from a compliance manager and a quality assurance specialist.

5.4.1. Results from the Questionnaire

The company is listed on Nasdaq and has many subsidiaries and sites around the world. The design and production departments are certified to ISO 13485 [6] and ISO 14001 [11]. There is good knowledge of the company's legal environment. Written ISO management system policy documents exist where safety and environmental risk is addressed. A formal risk management system is in place that covers both the design department and the production department. The risk management system is supported by a proposal system and work request management system. Risk assessment and risk analysis is conducted in a formal way. Internal audits are conducted. There is a management review process in place. ISO 14971 [42] is used as risk management guidelines to medical devices together with IEC 62366-1 [43] guidelines for application of usability engineering to medical devices. They are both referenced in ISO 13485. Risk is assessed regarding hazards, likelihood or probability, and consequence. Risk management includes continuous improvements, risk mitigation, cost analysis, documentation, and a risk-learning process. The efficacy of risk controls is evaluated. Risk criteria are set, and residual risk is assessed. Results from risk assessments are documented and used to learn from them.

5.4.2. Results from the Interview

The project manager was interviewed. Experts working in the design department were also interviewed to fill in gaps. The project manager explained the complicated design and production processes of the microcomputer-controlled device. There are numerous things that need to be considered, e.g., the clinical needs, the patient safety, human error, and fulfillment of the user requirements. Development of new products follows a detailed product development process for new products where every step, milestone, and gate of the process is defined. Records regarding every product are kept for seven years after cessation of production. Medical devices are subject to extensive regulations to assure patient safety. The devices are divided into risk categories and classes, with different regulatory requirements. This classification is not internationally standardized, e.g., Europe, USA, and Canada all use different classification. Risk management is fundamental in demonstrating regulatory compliance for medical devices and it is a fundamental part of manufacturing processes in the medical device industry. Risk management for the product was based on a top-down Failure Modes Effects and Criticality Analysis (FMECA).

The guidelines for risk management for medical devices mostly come from ISO 14971 and IEC 62366-1, both referenced in ISO 13485. Neither ISO 13485 nor IEC 62366-1 refer to ISO 31000, but ISO 14971 does. ISO 14001, however, only refers to ISO 31000 for risk management guidelines. There is a difference in the core concepts and nomenclature of ISO 14971 and ISO 31000 that has caused confusion. Example 1: ISO 31000 defines “event” as “occurrence or a change of a particular set of circumstances” while ISO 14971 leaves event undefined. Example 2: “harm” is defined as “injury or damage to the health of people, or damage to property or the environment” while ISO 31000 leaves it undefined and unmentioned. Example 3: “risk” is defined as “effect of uncertainty on objectives” in ISO 31000, but “combination of the probability of occurrence of harm and the severity of that harm” in ISO 14971. Example 4: “risk management” is defined as “coordinated activities to direct and control an organization with regard to risk” in ISO 31000, but “systematic application of management policies, procedures and practices to the tasks of analyzing, evaluating, controlling and monitoring risk” in ISO 14971.

In the opinion of the project manager, ISO 31000 offers a generic and abstract description of risk analysis but does not provide guidance on how to conduct it as such. ISO 14971 defines the risk analysis process for medical devices in four steps: (1) Intended use and reasonably foreseeable misuse; (2) identification of characteristics related to safety; (3) identification of hazards and hazardous situations; (4) risk estimation. The guidance ISO 14971 provides is, however, limited, e.g., “For each identified hazardous situation, the manufacturer shall estimate the associated risk(s) using available information or data. For hazardous situations for which the probability of the occurrence of harm cannot be estimated, the possible consequences shall be listed for use in risk evaluation and risk control”. It still mentions several risk analysis methods in appendices, and the manufacturer is supposed to select the appropriate method. Guidance is given on risk identification in ISO 31000, but not mentioned in ISO 14971.

The manufacturing company used ISO standards to structure the risk management system. The risk analysis is embedded into every part of the product development phase. The risk analysis is a teamwork and the technique used has been developed within the company over time. Although it is based on ISO 14971, it also uses templates and classification systems specially designed and applicable to the production of medical devices. A risk ranking system is used for evaluation of suppliers. Process risk analysis is also done for the optimization of business processes and better utilization of raw material and components. The design of new bionic products is based on knowledge from previous products, but innovation is also an important factor. When analyzing risk, the focus is mainly on known hazards. The risk of a bionic device is related to (a) the mechanical structure and stability; (b) the bionic part that must not give electric shocks; and (c) software that does not fail. An event does not always have the same consequence. In case of the medical device in this study, the hazardous situations can vary, e.g., a person can fall on the ground or fall

in stairs, and so the severity level can also vary. The likelihood of an incident occurring is examined, followed by analysis of the incident severity. According to ISO 14971, the risk analysis process is a control process, i.e., the risk analyst shall identify what could happen that might form a hazard, then mitigating controls are selected. The manufacturer defines the acceptable risk and documents the process and communication of the results.

A Risk Priority Number (RPN) is calculated, based on severity of risk and likelihood of occurrence. It is challenging for the risk analysts to evaluate these factors. The RPN must meet predefined risk criteria for the development to continue. The key to an acceptable RPN is to neither overdesign nor overengineer safety because it is expensive. At regular intervals in the development process, there is an approval milestone or gate, and the product must pass certain gate criteria. At each gate, the result of the risk analysis is reviewed by an experienced person outside the risk analysis team but with good understanding and overview of the operation. If test results are good, it indicates that the product meets the requirements, and the severity factor should therefore decrease.

MS Word tables and Excel sheets are used for registering the risk analysis information which are then saved in a risk analysis file. An initial copy of the risk analysis file is saved when the product is launched, and a history log is kept for traceability. If an incident occurs after marketing the product, data are added to the risk analysis file and saved with a new version number. The update of the risk analysis can mean increase of risk because of defects in the medical device or decrease of risk because the use of the device is successful. Detection of hazards related to the use of the medical device is the most challenging thing in the risk analysis. The challenge is not only to detect foreseeable misuse, but furthermore to identify and analyze risk associated with such misuse.

5.4.3. Summarized Results from the Manufacturing Company

In this study, the development and production of only one medical device was analyzed, not the whole business. It has taken the company many years to optimize their manufacturing processes for bionic medical devices. Safety must be built into the design and risk must be managed throughout both design and production phases. The whole process is based on continuous and iterative risk analysis. Risk analysis experts have gone to great lengths in their risk analysis to develop safe products and meet the requirements of regulators. The risk control system has been a burden at times, where regulators demand ever-increasing formality and documentation. Now, a balance in the cost effectiveness and the regulatory compliance has been reached. Applying ISO standards is one way of meeting requirements from regulators, supervising authorities, and buyers (that are typically not end-users). Despite limited guidance on risk management in ISO standards and inconsistency in their definition of important risk terms, the ISO standards are essential for the business. Table 7 presents a summary of the results from the development and production of a medical device. No issues were reported for benchmarks no. 5, 6, and 8 in the table. This means that the hypothesis could not be verified.

Table 7. Results from the manufacturing company.

No.	Benchmark	Issues found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	No issues reported	Not verified
6	Risk assessment ability to capture risk evaluation	No issues reported	Not verified
7	Risk criteria setting in risk assessment	No issues found	False
8	Treatment of residual risk	No issues reported	Not verified

During the interview with the product manager, he raised the question: “Is the company perhaps doing too much on risk analysis and risk management?” He further stated that “risk management can easily go overboard, but the thin line to follow is to catch and deal with relevant risk without spending too many resources”.

5.5. Software Company

The software company (organization E in Table 2) develops risk management software for an international client base, a modular software suite. It also provides hosting services and information technology consultancy. The software is a database hybrid (client-server and web-based) solution. It is mainly used by organizations for their business activities, but also for training and education at universities. The company is focused on innovation and collaboration with universities. It has received European project grants for the development of the software.

5.5.1. Results from the Questionnaire

The software company is listed on Nasdaq and has one subsidiary. All its business activities are certified to ISO/IEC 27001 [3]. There is good knowledge of the legal environment. Written information security policies exist, supported by other policies, e.g., access policy and teleworking policy. A formal risk management process is in place. Risk assessment and risk analysis is conducted, there is internal control, regular internal and external audits, and a management review process. Risk management software is used with a built-in risk analysis module. Risk is associated with both tangible and intangible assets. Threats to assets are identified, and consequence of risk is assessed. Likelihood of risk is a factor in the assessment and risk is calculated. Residual risk is assessed, and risk criteria are set. Risk is monitored, reviewed, and treated. Effectiveness of controls in terms of cost is not evaluated. Results from risk assessment are documented and used to learn from them.

5.5.2. Results from the Interview

The security manager of the software company explained that changes in ISO/IEC 27001 since 2005 have been confusing. The focus was on asset-based risk assessment methodology, but in the latest version, ISO/IEC 27001:2013, there is only mention of assets in Annex A. The referenced guidelines on risk management are ISO/IEC 27005 [44] and ISO 31000 [12]. There is a difference in the core concepts and nomenclature of ISO 31000 and ISO/IEC 27005. When it comes to risk analysis, ISO 31000 offers a generic and general risk management guidance but no guidance on how to conduct risk analysis as such. ISO/IEC 27005 offers limited guidance on how to conduct risk analysis, for example: (a) risk analysis depends on the criticality of assets; (b) it is based on assessed consequence and likelihood; (c) it can be done on a qualitative or a quantitative scale. The software company uses a combination of qualitative and quantitative risk assessment techniques built in a software solution.

The risk assessment is conducted in line with ISO/IEC 27001. It is based on assets, both tangible and intangible, and their properties in terms of value, confidentiality, integrity, and availability. Potential threats to assets and asset vulnerabilities are identified and assessed. Three risk calculations are made for every asset:

1. Inherent risk factor, the base security risk, is calculated for every asset based on four variables: the likelihood of threat, the impact of threat, the vulnerability of the asset towards the threat, and the value of the asset of which the threat is associated with. All four variables are evaluated on a scale between 1 and 5.
2. The second risk calculation is the current security risk. Risk is calculated with regard to implemented controls. A threat library is used in this calculation. Every threat is related to several controls from ISO/IEC 27001 which are meant to mitigate it. A calculation is made that considers, on the one hand, controls that are already implemented and, on the other hand, controls that have been defined as possible but

- have not yet been implemented. This gives a risk factor that can be compared to the inherent risk factor to assess the benefits of the measures that have already been taken.
3. The third risk calculation is similar to the second risk calculation. It takes into consideration both implemented and future controls, i.e., controls which are being considered or have already been chosen to be implemented but have not yet been implemented. This calculation is made to evaluate the benefit of future controls.

Description of risk is written in a free-text fields, but history of risk changes is difficult to verify. The causal relationship of complex risk is not captured. Although risk criteria are set as numbers, the meaning of the numbers remains unclear. The efficacy and maturity of the controls (mostly taken from ISO/IEC 27001) are difficult to comprehend.

Through their international client base, mostly ISO certified organizations, the software company is aware of the limitations of ISO standards when applied to analyze and manage risk in challenging operations. The security manager pointed out that ISO standards provide little guidance on how to analyze and assess risk. Therefore, the company risk analysts have conducted their own studies based on state-of-the-art literature and collaborated with academic experts in the risk field. The aim has been to find methods to better capture and manage risk that arises from complex interactions and emergent behavior that is inherent in present-day socio-technical systems. Thus, systems theory methods (<https://www.sciencedirect.com/topics/psychology/systems-theory>, accessed on 9 March 2022) have been investigated and Systems-Theoretic Process Analysis (STPA) technique has been used [45,46]. In this way, risk factors have been identified that could not be identified with previous methods based on ISO/IEC standards. By the end of this case study, the software company already conducted its risk analysis in two ways, for comparison, in line with ISO standards and with the STPA technique. With STPA, risk and causal relationships were identified that had not been identified before, e.g., risk regarding company merger, lawbreaking of employees, breaches of confidentiality, industrial disputes, strikes, pandemic, and technology transitions.

5.5.3. Summarized Results from the Software Company

The results from the questionnaire are based on the certified ISO risk management system. The use of the systems theory method, STPA, has not yet been fully implemented in the risk analysis process. The use of risk management software ties the risk assessment, risk analysis, and the risk treatment to requirements and controls from ISO/IEC 27001. Risk calculations are performed in three ways to clarify and support risk management decisions. Various information is registered in free-text fields regarding asset properties, threats, likelihood, and vulnerabilities. This is to ensure that different parties within the company can assess the risk based on the same information and come to the same conclusion regarding risk. Despite the effort and the good awareness of the company's experts, it is their own assessment that various risk issues are present. Table 8 presents a summary of the results from the software company. It shows that only benchmarks no. 1 and 3 are without any issues.

Table 8. Results from the software company.

No.	Benchmark	Issues Found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	Fales
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Internal boundaries sometimes unclear	True
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	Lack of resources	True
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Limited ability to capture risk evaluation	True
7	Risk criteria setting in risk assessment	Risk setting unclear	True
8	Treatment of residual risk	Residual risk partly addressed	True

5.6. Pension Fund

The pension fund (organizations F in Table 2) has a governmental operating license and is subject to official supervision. The pension fund places great emphasis on risk analysis in its investments and the financial crisis in 2008 did not have a significant adverse effect on it. The fund did not have to reduce pension rights after the financial crisis. The investments are international, in bonds, equities, and mortgage loans for members. During the time of this study, the pension fund implemented a formal management system according to ISO management system standards. This was partly done to reinforce trust, but also to meet stricter regulatory requirements after the financial crisis.

5.6.1. Results from the Questionnaire

All the pension fund's business activities are certified to ISO/IEC 27001 [3] and ISO 9001 [2]. There is good knowledge of the legal environment. Written information security and quality policies exist. They are supported by other policy documents, e.g., risk policy and investment policy. A formal risk management process is in place. This means that risk assessment and risk analysis is conducted. There is internal control, regular audits (internal and external), and a management review process. Risk analysis is conducted, a formal risk analysis technique is used and recorded in Excel templates. Risk is associated with assets, both tangible and intangible. Threats to assets are identified, and consequence of risk is assessed. Likelihood of risk is a factor in the assessment and risk is calculated. Residual risk is assessed, and risk criteria are set. Risk is monitored, reviewed, and treated, efficacy of controls in terms of cost is not evaluated. Results from risk assessment are documented and used to learn from them.

5.6.2. Results from the Interview

The CEO of the pension fund was interviewed. He revealed that his participation in this study was a part of the pension fund's risk management reinforcement. All business procedures were reviewed during the time of this study with regard to requirements in ISO management system standards. The risk assessment process and risk analysis itself was also strengthened. External experts were hired to work with the management team and the board of directors. They submitted reports with forecasts and analyses. An advisory board including foreign experts was established.

A quarterly risk management report is prepared for the board based on the asset position. The report also includes analysis of financial changes, investment policy, currency development, economic forecast and prospects, breakdown of asset categories, return on assets over different periods of time (also categorized), Q/A on the asset portfolio, and overview of risk factors. The risk analysis, risk evaluation, and risk calculation are made in an Excel sheet that contains an overview of risk factors and risk calculations:

1. Basic risk score = ((impact of risk) × (likelihood of risk)) + (impact other than financial)
2. Quarterly risk score = (basic risk score) – ((effectiveness of mitigating control) × (basic risk score))
3. Previous quarterly risk score
4. Involvement of pension fund division
5. Responsible division
6. Description of risk factors
7. Possible consequences of risk
8. Description of mitigation controls
9. Objectives
10. Comments
11. Reference to a documented process

The risk score calculation is based on a two-dimensional risk matrix: x = impact of risk (on scale 1–7); y = likelihood of risk (on scale 1–4). Identified risk factors have remained the same over time.

At the end of this study, all work processes and procedures had been documented and linked to requirements in ISO standards ISO 9001 and ISO 27001. Standard requirements had also been analyzed in conjunction with departments. The development of risk analysis techniques continues and is not based on ISO standards. Awareness of societal and technological changes has reinforced managers' determination to analyze risk even better than before. Ways are being sought to further deepen the understanding of the risks associated with individual investment opportunities, especially those based on complex technologies.

5.6.3. Summarized Results from the Pension Fund

The pension fund's risk experts consider themselves well aware of financial and investment risk factors. This is confirmed by the fund's good performance in previous years. However, some risk factors have not been identified, e.g., risk associated with hybrid threats and world threats, such as pandemics, environmental threats, democratic threats, technology transition (e.g., blockchain), and international politics. Future international investments require risk to be carefully assessed and aligned with the investment policy. Not only the expected return on investment must be considered, but also requirements from members regarding sustainability, environmental impact, and ethics. Therefore, the risk analysis must not only be transparent, dynamic, and efficient, it must also be reliable and systematic in capturing new risk factors arising from present-day complex systems. Table 9 presents a summary of the results from the pension fund investments.

Table 9. Results from the pension fund.

No.	Benchmark	Issues found	Hypothesis (True/False)
1	Scope and outer boundaries of a RM system	No issues found	False
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	No issues found	False
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	No issues found	False
4	Resources available to support the RM system	No issues found	False
5	Risk analysis ability to capture complex systems and business operations	Limited ability to capture complexity	True
6	Risk assessment ability to capture risk evaluation	Risk assessment ability to capture risk evaluation is limited	True
7	Risk criteria setting in risk assessment	Risk criteria unclear	True
8	Treatment of residual risk	Treatment of residual risk unclear and residual risk not always addressed	True

6. Discussion

The aim of this study was twofold, to develop a benchmarking model for risk management and to test it on six real-life and ISO-certified risk management systems.

6.1. First Aim: Development of a Benchmarking Model for Risk Management

The results of the study show that it can be difficult to assess the efficacy of risk management, even if the risk management system is ISO-certified. The certification is not a guarantee of being able to identify and assess all relevant risks in business operations. Methods and tools are needed to support evaluation of the efficacy and robustness of a risk management system. The two-step benchmarking model developed in this study can be used as a tool for this purpose and leaves opportunities for further development. The model uses an assessment template with a simple scoring system to verify and evaluate all main parts of a risk management systems. If the evaluation is positive and the risk management system proves to have all necessary parts in it, the next step is to dive deeper and assess the efficacy of individual parts of the system. Risk analysis and risk assessment are two of the most challenging parts for many organizations. These parts need to be examined

and evaluated regarding the ability to detect risk, often in complex systems. In this study, the participants assessed their own risk management systems through a questionnaire. The answers were supported by documents of various kind. After reviewing the answers and documents, interviews were conducted as audit meetings to verify all information provided. Step 2 in the benchmarking model was applied to capture qualitative data. The scoring was in the form of “risk issues found”.

The study shows that it is important to build the benchmarks on risk science. Further research is needed to find out whether it is possible to develop a standardized scoring system based on risk science that serves as a good indicator of evaluation ability. There are also other aspects of risk management that need to be considered, for example, identification of risk leading indicators. Recent research has been conducted in this area [47]. The overall efficacy of the risk management system needs to be further examined. To handle complexity, robustness and resilience must also be addressed. More such factors need to be analyzed and ways found to measure and evaluate them.

Recent literature on risk management describes the importance of benchmarking models for improvements and quality assurance. The literature also describes various risk issues and challenges faced when managing risk in complex socio-technical systems. Several approaches to systems thinking have been proposed to understand such systems. These approaches may increase system and risk understanding but may still need to be supplemented with other approaches to adequately support risk management. Better modeling is advocated and qualitative modeling tools with description of systemic behavior are recommended for identification and evaluation of risk in complex systems. ISO 31000 neither addresses the importance of risk models nor describes how to go about creating such models.

6.2. Second Aim: Application of a Benchmarking Model for Evaluation of Real-Life ISO Risk Management Systems

The study shows that ISO standards can be applied in many ways in risk management systems, depending on the nature of the operation and the business needs. Evidence, results, and testimonials in this study confirm that risk management is increasingly important for business, and it is becoming an integrated part of a management system. This is in line with findings in a former study [8]. The study also shows that in all six cases examined, different approaches are taken to risk analysis and risk management. By applying the benchmarking model developed in this study, it was possible to find both risk issues and risk factors that had not previously been found.

The study provides evidence that despite the importance and good efforts, risk management and particularly the analysis of risk was not done satisfactorily in four out of six cases studied. Table 10 gives an overview of the risk issues found and in which organizations. The first two columns show the number and the name of the benchmarks. The third column shows the correspondence of the benchmarks to the three parts of the ISO 31000 risk management guidelines, i.e., principles, framework, and process. Columns 4–9 show the findings in the organizations’ risk management system. The last column shows the frequency of risk issues found based on benchmarking. The “x” means that issues were found in the risk management system, “ ” (a blank) means that no issues were found, “(*)” means that risk issues could not be completely verified in this study. The last column shows the frequency of the risk issue (max 6). At the bottom of the table, the total number of risk issues found in every case is shown, max 8 risk issues in every organization A–F.

Table 10. Overview of the risk issues found and in which organizations.

No.	Benchmark	Corresponding to Risk Management (RM) in ISO 31000:2018	Risk Issues Found						Frequency of Risk Issues
			A—Public Health Service	B—Public Supply System	C—Construction Company	D—Manufacturing Company	E—Software Company	F—Pension Fund	
1	Scope and outer boundaries of a RM system	Process: Scope, context, and criteria	x	x					2
2	Interfaces (internal boundaries, departments, unclear responsibility) within a RM system	Process: Scope, context, and criteria	x	x				x	3
3	Hierarchical issues (layer issues, unclear hierarchical safety, and security structure) within a RM system	Principles: Structured, comprehensive, and dynamic Framework: Leadership and commitment Process: Risk assessment and treatment		x					1
4	Resources available to support the RM system	Framework: Leadership and commitment		x				x	2
5	Risk analysis ability to capture complex systems and business operations	Process: Risk assessment	x	x	n.v.	n.v.	x	x	4
6	Risk assessment ability to capture risk evaluation	Process: Risk assessment	x	x	n.v.		x	x	4
7	Risk criteria setting in risk assessment	Process: Risk assessment and treatment	x	x	n.v.	n.v.	x	x	4
8	Treatment of residual risk	Principles: Continual improvements Framework: Improvement Process: Risk assessment, treatment, monitoring, and review	x	x	n.v.	n.v.	x	x	4
Total no. of risk issues found in RM system			6	8			6	4	24

"x" = risk issues found; "" = no risk issues found; "n.v." = could not be verified in this study.

This can be summarized as follows:

1. Scope and outer boundary issues were found in 2 out of 6 cases.
2. Interface issues were found in 3 out of 6 cases.
3. Hierarchical issues were found in 1 out of 6 cases.
4. Resource issues were found in 2 out of 6 cases.
5. Issues regarding risk analysis ability to capture complex systems and business operations were found in 4 out of 6 cases.
6. Issues regarding risk assessment ability to capture risk evaluation were found in 4 out of 6 cases.
7. Issues regarding setting of risk criteria were found in 4 out of 6 cases.
8. Issues regarding residual risk were found in 4 out of 6 cases.

Risk issues were identified in four out of six risk management systems. In the other two risk management systems, risk issues could not be completely verified (still marked as "No issues found"), which does not mean that risk issues did not exist at some point. Review of these findings with correspondence to the risk management description in ISO 31000:2018 (see Table 1) shows that there is weakness in the risk management principles, the framework,

and the process (see Figure 1). In view of the previous study, this is a clear indication of a lack of guidance on risk management and inconsistency in risk terminology in ISO standards, as demonstrated in [8].

Testimonials confirm that all the organizations are searching for better and more efficient risk analysis methods; a systematic method that provides better risk finding assurance. Common causes for risk factors are often not identified because of boarder and interface issues, complexity issues, and lack of overview. One of the reasons is the frequently used bottom-up approach in risk assessments, where different departments assess their own risk and then risk information is compiled into one risk register (risk library) without further risk analysis. Emergent behavior, time lags, and relevant control or feedback loops are not identified through the risk management approach in any of the cases.

The risk management systems of the construction company (organization C) and the manufacturing company (organization D) proved to be satisfactory for the two projects analyzed in this study, a construction of one infrastructure facility and the development of one medical device. Despite being very different, both management systems are mature and based on many years of experience. During the construction phase of the construction facility, no guidance from ISO standards was used. The manufacturer of medical devices developed a risk management system for the development of medical devices that uses ISO standards as a basis, but the risk analysis technique was developed by risk experts within the company, where experience and knowledge of the design and production of medical devices has a long history. The manufacturer of medical devices tries to capture risk related to user errors of the medical device. The software company (organization E) is the only case where systems theory has been applied, but only for a short time. It is still being tested but the company has managed to improve its identification and analysis of risk with help of the STPA technique [45,46].

Although it has not been specifically analyzed, it is obvious that the organizations in this study have invested significantly in their risk management systems. Once an accredited certification has been obtained, there is increased reputational and image risk involved in losing or giving up the certification. The support from top management is important, not only to establish the risk management system, but also to maintain it. It is understandable that people want to keep risk analysis as simple as possible. If a simple analysis has been done and it has been helpful, there is a reluctance to increase complexity, especially at increased cost. When is it necessary to take the next step? The decision is easier if a simpler and more cost-effective new method is found. Even then, regulatory requirements must be fulfilled.

During the time of the study (2014–2019) efforts to improve risk analysis were evident by the public supply system (organization B), the software company (organization E), and the pension fund (organization F). However, unsubstantiated methods are used, such as two-dimensional risk matrices, by all organizations except the software company. That company has been certified to ISO/IEC 27001 since 2004 and specialization in the risk field has driven knowledge and led to maturity of its risk management process which nevertheless has risk issues. All interviewees in this study noted that risk assessment, including risk analysis, has been a demanding and difficult task for them. Communicating results from risk assessments to either internal parties (e.g., board of directors) or external parties (e.g., governmental authorities), is also challenging. It was argued that especially third-party organizations (e.g., regulators, contractors, suppliers) did not always understand the effort associated with risk management. It was also argued that these parties lack an understanding of the complexity of risk management and the time and cost involved. This again increases risk.

7. Conclusions and Future Work

In this article, we have investigated how benchmarking theory can be combined with risk science and used to gain and improve understanding of the efficacy of a certified ISO

risk management systems in real business operations. It was hypothesized that although organizations have certified ISO risk management systems, certain flaws in risk management would be evident in practice, assuming that the representatives of the organizations in this study are describing the true situation in their organizations. The findings presented in Section 5 show that this is clearly the case in four out of six risk management systems, also shown in an overview in Table 10, cases A (with 6 types of risk issues), B (with 8 types of risk issues), E (with 6 types of risk issues), and F (with 4 types of risk issues). In the other two systems, C and E, this could not be verified, but risk issues could not be ruled out. Table 10 also reveals general weaknesses in risk analysis ability, risk assessment ability, setting of risk criteria, and treatment of residual risk. These are critical issues for managing risk in complex socio-technical systems.

In relation to the identification of hidden risk of organizations through the ISO standards-based risk management system, it was found that with the benchmarking model, more risk factors can be found without any significant changes to the risk identification and risk assessment processes. The benchmarking model in this study belongs to cross-sectoral type of benchmarking and it clearly helps identifying hidden risk, for example, risk associated with hybrid threats and world threats (such as pandemics), environmental threats, democratic threats, technology transition, and international politics. Although no defects of the model were observed during its use the model needs further refinement. It is adapted to ISO 31000, but the measurability of individual benchmarks needs further development in connection with use in diverse operations. For example, in this study, the measurement of risk criteria setting, and the treatment of residual risk consisted primarily in confirming that these factors were addressed. The way in which they were handled was examined but it was not possible to measure how effective the controls are. In order for this to be possible, the measurability needs to be investigated further and measurement techniques need to be developed.

All the organizations evaluated in this study have extensive experience in the use of ISO standards and showed both understanding and commitment in risk management. They all rely heavily on the risk management guidelines in ISO standards. They are all aware of weaknesses in their risk analysis techniques and acknowledge that it is partly due to inadequate guidance in the standards. With help of the benchmarking tool developed in this study it was possible to identify flaws in four out of six systems analyzed. Although no issues were reported in two out of six systems, the benchmark model identifies possible weaknesses that need to be further analyzed. This presents opportunities for improvement. It appears that all organizations are willing to change their approach to risk analysis if a better technique is found in the sense of uncovering risk that has previously been unidentified, being efficient, not too complicated, not manpower intensive, and not too expensive.

The limitation of this research lies in the data available, time required to analyze data, experts' knowledge needed to evaluate the data, an understanding of specific and complex systems, and changes that occur in perpetual systems over time. The weakness of the risk analysis conducted in this study lies in the measurability of both risk and efficacy of risk management. This is difficult to standardize, and every organization must find an appropriate risk analysis technique where causal relationship of risk factors, risk criteria, risk acceptance, and residual risk can be made understandable and measurable. It would be of great value if ISO standards contained better guidance to help and support their users in this continuous process.

The findings, however, show that there is a strong reason to further investigate the measurability of effectiveness in operation risk management systems. This is a subject for future work. The practical implications of the study are of value for company managers, risk analysts, and those who develop standards, e.g., ISO. This study also contributes to benchmarking theory and highlights the challenging task to measure qualitative risk factors, being able to define measurable risk factors and having the right measure to assess the risk. It reveals the importance of building risk management systems in organizations on a risk

science foundation. As future work, the authors plan to further develop the benchmarking model based on recent risk science literature and to test the model in more organizations.

Societies are undergoing a huge change, often referred to as the fourth industrial revolution (<https://www.weforum.org/focus/fourth-industrial-revolution>, accessed on 9 March 2022). This means increasing automation and a revolution in the use of digital solutions by people and organizations. This development is intertwined with, e.g., biotechnology, environmental issues, and sustainability requirements. This change can provide great benefits to societies. However, these developments bring new and previously unknown risks and threats, e.g., to nature, democracy, humanity, and health. According to the Global Risks Report 2021 and 2022, published by the World Economic Forum, the COVID-19 pandemic has accelerated this revolutionary change [48,49]. Such risks are not a private business matter, such as a quality of a product or a service, and cannot be treated as a strategic variable within an organization (like quality). Therefore, behind the decision of an organization to take risk, there should be consideration of many aspects of potential positive or negative consequences.

For the forthcoming changes to be successful and beneficial for societies and businesses, a constructive risk culture must be created within businesses, such that important decision making is well thought through and supported by risk analysis. Solid risk analysis must become inevitable in all management and decision making. ISO standards are an important foundation to build on. However, if the risk management guidelines of ISO standards are inappropriate, there is a high risk that they will not achieve their aim to support and strengthen businesses. Previous research [8] confirms the lack of guidance in ISO standards in risk analysis, especially regarding risk in complex socio-technical systems. To redress this, ISO should review its business strategy and base the guidelines more on risk science, for example, through active collaboration with organizations like the Society for Risk Analysis (<https://www.sra.org/>, accessed on 9 March 2022).

Author Contributions: S.H.B. conducted the research, led the study, and arranged the paper in the present conceptualization form. P.J. supervised the research and contributed to the writing and review. S.E.T., I.M.D. and R.J.d.B. contributed to writing, review, and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved in accordance with the requirements of the Institutional Review Department of Reykjavik University (RU-DoE-Review-Board-Oct 2021, 28 October 2021).

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank the six organizations and their representatives for participating in this study. Thanks for sharing their hazard and risk analysis and for the inspiring risk-related discussions. Their interest, integrity, and support made this study an informative and pleasant journey that lasted five years. Thanks also to the reviewers of this article and their valuable comments.

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

References

1. COPOLCO. 2021. Available online: https://www.iso.org/sites/ConsumersStandards/1_standards.html (accessed on 15 February 2021).
2. *ISO 9001:2015*; Quality Management Systems—Requirements. ISO: Geneva, Switzerland, 2015.
3. *ISO/IEC 27001:2013*; Information Technology—Security Techniques—Information Security Management Systems—Requirements. ISO: Geneva, Switzerland, 2013.
4. *ISO 45001:2018*; Occupational Health and Safety Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/37/63787.html> (accessed on 9 March 2022).

5. ISO 22000:2018; Food Safety Management Systems—Requirements for any Organization in the Food Chain. ISO: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/54/65464.html> (accessed on 14 July 2020).
6. ISO 13485:2016; Medical Devices—Quality Management Systems—Requirements for Regulatory Purposes. ISO: Geneva, Switzerland, 2016.
7. ISO 37001:2016; Anti-Bribery Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2016. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/50/65034.html> (accessed on 9 March 2022).
8. Björnsdóttir, S.H.; Jensson, P.; de Boer, R.J.; Thorsteinsson, S.E. The Importance of Risk Management: What is Missing in ISO Standards? *Risk Anal.* **2021**. [[CrossRef](#)] [[PubMed](#)]
9. International Accreditation Forum, Inc. International Accreditation Forum—IAF. *Find Members, Publications & Resources*. 13 July 2020. Available online: <https://www.iaf.nu/> (accessed on 7 September 2020).
10. ISO—Management System Standards List. Available online: <https://www.iso.org/management-system-standards-list.html> (accessed on 9 July 2020).
11. ISO 14001:2015; Environmental Management Systems—Requirements with Guidance for Use. ISO: Geneva, Switzerland, 2015.
12. ISO 31000:2018; Risk Management—Principles and Guidelines. ISO: Geneva, Switzerland, 2018.
13. ISO 19011:2018; Guidelines for Auditing Management Systems. IEC: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/00/70017.html> (accessed on 20 July 2020).
14. Talapatra, S.; Uddin, M.K.; Rahman, M.H. Development of an Implementation Framework for Integrated Management System Based on the Philosophy of Total Quality Management. *Am. J. Ind. Bus. Manag.* **2018**, *8*, 6. [[CrossRef](#)]
15. Talapatra, S.; Uddin, M.K. Prioritizing the barriers of TQM implementation from the perspective of garment sector in developing countries. *Benchmarking Int. J.* **2019**, *26*, 2205–2224. [[CrossRef](#)]
16. Franceschini, F.; Galetto, M.; Cecconi, P. A worldwide analysis of ISO 9000 standard diffusion: Considerations and future development. *Benchmarking Int. J.* **2006**, *13*, 523–541. [[CrossRef](#)]
17. Herbst, N.; Bauer, A.; Kounev, S.; Oikonomou, G.; Eyk, E.V.; Kousiouris, G.; Evangelinou, A.; Krebs, R.; Brecht, T.; Abad, C.L.; et al. Quantifying Cloud Performance and Dependability: Taxonomy, Metric Design, and Emerging Challenges. *ACM Trans. Model. Perform. Eval. Comput. Syst.* **2018**, *3*, 1–36. [[CrossRef](#)]
18. Kounev, S.; Lange, K.-D.; von Kistowski, J. *Systems Benchmarking: For Scientists and Engineers*; Springer International Publishing: Cham, Switzerland, 2020. [[CrossRef](#)]
19. Olawumi, T.O.; Chan, D.W.M. Development of a benchmarking model for BIM implementation in developing countries. *Benchmarking Int. J.* **2019**, *26*, 1210–1232. [[CrossRef](#)]
20. Van der Voordt, T.J.M.; Jensen, P.A. Measurement and benchmarking of workplace performance: Key issues in value adding management. *J. Corp. Real Estate* **2018**, *20*, 177–195. [[CrossRef](#)]
21. Staiger, R.D.; Schwandt, H.; Puhani, M.A.; Clavien, P.-A. Improving surgical outcomes through benchmarking. *Br. J. Surg.* **2019**, *106*, 59–64. [[CrossRef](#)]
22. Hartono, E.O.; Abdullah, D. HFLTS-DEA Model for Benchmarking Qualitative Data. *Int. J. Adv. Soft Comput. Appl.* **2019**, *11*, 109–131.
23. Mangla, S.K.; Luthra, S.; Jakhar, S. Benchmarking the risk assessment in green supply chain using fuzzy approach to FMEA: Insights from an Indian case study. *Benchmarking Int. J.* **2018**, *25*, 2660–2687. [[CrossRef](#)]
24. Hoffmann, P.; Schiele, H.; Krabbendam, K. Uncertainty, supply risk management and their impact on performance. *J. Purch. Supply Manag.* **2013**, *19*, 199–211. [[CrossRef](#)]
25. Björklund, M. Benchmarking tool for improved corporate social responsibility in purchasing. *Benchmarking Int. J.* **2010**, *17*, 340–362. [[CrossRef](#)]
26. Moriarty, J.P.; Smallman, C. En route to a theory of benchmarking. *Benchmarking Int. J.* **2009**, *16*, 484–503. [[CrossRef](#)]
27. MacGillivray, B.H.; Sharp, J.V.; Strutt, J.E.; Hamilton, P.D.; Pollard, S.J.T. Benchmarking Risk Management Within the International Water Utility Sector. Part II: A Survey of Eight Water Utilities. *J. Risk Res.* **2007**, *10*, 105–123. [[CrossRef](#)]
28. Talapatra, S.; Uddin, M.K.; Antony, J.; Gupta, S.; Cudney, E.A. An empirical study to investigate the effects of critical factors on TQM implementation in the garment industry in Bangladesh. *Int. J. Qual. Reliab. Manag.* **2019**, *37*, 1209–1232. [[CrossRef](#)]
29. Talapatra, S.; Uddin, K. Understanding the difficulties of implementing TQM in garment sector: A case study of some RMG industries in Bangladesh. In Proceedings of the International Conference on Mechanical, Industrial and Materials Engineering 2017 (ICMIME2017), Rajshahi, Bangladesh, 28–30 December 2017; p. 6. Available online: <http://icmime-ruet.ac.bd/2017/DIR/Contents/Technical%20Papers/Industrial%20Engineering/IE-243.pdf> (accessed on 1 November 2021).
30. Talapatra, S.; Uddin, K. *Some Obstacles that Affect the TQM Implementation in Bangladeshi RMG Sector: An Empirical Study*; IEOM Society International: Bandung, Indonesia, 2018; p. 13. Available online: <http://ieomsociety.org/ieom2018/papers/401.pdf> (accessed on 9 March 2022).
31. Aven, T.; Zio, E. Foundational Issues in Risk Assessment and Risk Management. *Risk Anal.* **2014**, *34*, 1164–1172. [[CrossRef](#)]
32. Klinkle, A.; Renn, O. A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Anal.* **2002**, *22*, 1071–1094. [[CrossRef](#)]
33. Cox, L.A. What’s Wrong with Risk Matrices? *Risk Anal.* **2008**, *28*, 497–512. [[CrossRef](#)]




34. IEC 31010:2019; Risk management—Risk assessment techniques. IEC: Geneva, Switzerland, 2019.
35. Aven, T. Improving risk characterisations in practical situations by highlighting knowledge aspects, with applications to risk matrices. *Reliab. Eng. Syst. Saf.* **2017**, *167*, 42–48. [CrossRef]
36. Fellows, R.; Liu, A.M.M. Managing organizational interfaces in engineering construction projects: Addressing fragmentation and boundary issues across multiple interfaces. *Constr. Manag. Econ.* **2012**, *30*, 653–671. [CrossRef]
37. Mikes, A. From counting risk to making risk count: Boundary-work in risk management. *Account. Organ. Soc.* **2011**, *36*, 226–245. [CrossRef]
38. Zerjav, V. Design boundary dynamics in infrastructure projects: Issues of resource allocation, path dependency and problem-solving. *Int. J. Proj. Manag.* **2015**, *33*, 1768–1779. [CrossRef]
39. Lathrop, J.; Ezell, B. A systems approach to risk analysis validation for risk management. *Saf. Sci.* **2017**, *99*, 187–195. [CrossRef]
40. Blood Transfusion Guide—EDQM Publications | EDQM—European Directorate for the Quality of Medicines. 2020. Available online: <https://www.edqm.eu/en/blood-guide> (accessed on 29 April 2021).
41. WHO Action Framework to Advance Universal Access to Safe, Effective and Quality Assured Blood Products. 2020. Available online: <https://www.who.int/publications-detail-redirect/action-framework-to-advance-uas-bloodprods-978-92-4-000038-4> (accessed on 29 April 2021).
42. ISO 14971:2019; Medical Devices—Application of Risk Management to Medical Devices. ISO: Geneva, Switzerland, 2019. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/27/72704.html> (accessed on 9 March 2022).
43. IEC 62366-1:2015; Medical Devices—Part 1: Application of Usability Engineering to Medical Devices. IEC: Geneva, Switzerland, 2015.
44. ISO/IEC 27005:2018; Information Technology—Security Techniques—Information Security Risk Management. ISO: Geneva, Switzerland, 2018. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/52/75281.html> (accessed on 13 July 2020).
45. Leveson, N. A new accident model for engineering safer systems. *Saf. Sci.* **2004**, *42*, 237–270. [CrossRef]
46. Leveson, N.G. Engineering a Safer World. 2011. Available online: <https://mitpress.mit.edu/books/engineering-safer-world> (accessed on 3 July 2018).
47. Leveson, N. A systems approach to risk management through leading safety indicators. *Reliab. Eng. Syst. Saf.* **2015**, *136*, 17–34. [CrossRef]
48. The Global Risks Report 2021. *The World Economic Forum*. 2021. Available online: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (accessed on 12 April 2021).
49. The Global Risks Report 2022. *The World Economic Forum*. 2022. Available online: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (accessed on 9 March 2022).

Article C

Aligning Stakeholders and Actors: A New Safety and Security-Based Design Approach for Major National Infrastructures

Article

Aligning Stakeholders and Actors: A New Safety and Security-Based Design Approach for Major National Infrastructures

Svana Helen Björnsdóttir ^{1,*} , Pall Jenson ¹, Saemundur E. Thorsteinsson ², Ioannis M. Dokas ³ 
and Helgi Thor Ingason ¹ 

¹ Department of Engineering, Reykjavik University, 101 Reykjavík, Iceland; pallj@ru.is (P.J.); helgithor@ru.is (H.T.I.)

² Department of Engineering, University of Iceland, 101 Reykjavík, Iceland; saemi@hi.is

³ Department of Civil Engineering, Democritus University of Thrace, 69100 Komotini, Greece; idokas@civil.duth.gr

* Correspondence: svanahb@ru.is; Tel.: +354-899-9200

Abstract: This study introduces a systems-theoretic methodology to meet the requirements of a major national infrastructure for safety and security-based design by enhancing the alignment of stakeholders and actors in the project. Safe-by-Design (SbD) is an engineering concept for risk management that considers safety as much as possible in the design phase. The article presents the results of a case study conducted to investigate the efficacy of recent system safety models and analysis techniques in the major national infrastructure of a Waste-to-Energy (WtE) project under consideration in Iceland. The structures and roles within the system responsible for constructing the WtE plant, given the sustainability and circular economy restrictions, are addressed in the study. Stakeholders' roles and responsibilities are analyzed, yielding their feedback on potential risks and creating a positive image of the project. Also, suitable ways to enter the project and finance it are devised. In essence, this enables the creation of a safety and security-based design approach. Furthermore, detailed documentation of the system model development is presented. The novelty of the study lies in the application of STAM, STPA, and STECA as an SbD approach for a major infrastructure project. Also, the methods discussed here have not been used in a WtE project as far as we know.

Keywords: Waste-to-Energy; sustainability; circular economy; STAMP; STPA; STECA; risk analysis; project management; Safe-by-Design



Citation: Björnsdóttir, S.H.; Jenson, P.; Thorsteinsson, S.E.; Dokas, I.M.; Ingason, H.T. Aligning Stakeholders and Actors: A New Safety and Security-Based Design Approach for Major National Infrastructures. *Sustainability* **2024**, *16*, 328. <https://doi.org/10.3390/su16010328>

Academic Editor: Bin Xu

Received: 13 November 2023

Revised: 18 December 2023

Accepted: 26 December 2023

Published: 29 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

This study was conducted to investigate a relatively new methodology and techniques, still in development, for solving the objectives of a safety and security-based design of a major national infrastructure. The research objectives were tested on a specific project, a WtE project that can have significant and diverse impacts on people and the environment. It is feared that it may have many safety and security issues unless they are considered from the beginning, as well as risks being identified and met appropriately during decision making at all stages of the project from the start. The safety and security issues people fear are, e.g., harmful long-term effects on the health of people and nature in the vicinity of the incineration plant, odor pollution, smoke pollution, visual pollution, noise pollution, weight of traffic due to heavy transport with waste, carbon offsets, secure financing for construction and operation, and increased costs for the public and local authorities for waste disposal and treatment.

The project chosen for the analysis is at an early stage, and a detailed analysis and validation of all aspects is needed, i.e., assessment of the amount of waste to be incinerated in the coming decades, the size of the incinerator, and the scope of the entire project. Then, a suitable place needs to be selected for the incineration plant. It has to be designed in

accordance with the environment and nature of the place, and possible transport routes on land and at sea must be analyzed. Furthermore, technical solutions must be selected so that the incineration will be as efficient as possible, the cleaning process must be designed, and the associated cleaning equipment must be selected, together with various monitoring and warning systems, control systems, and automation of various kinds. When looking at all these factors, it is also important to assume a suitable ownership arrangement, such that those involved in the project from the beginning will have the means, the will, and the ability to build and operate a WtE incineration plant, so that they can live up to the responsibility they take on in the project. Various laws and regulations apply to this kind of project, including the EU market and competition laws, which affect the forms of businesses. There is, for example, a distinction made between the tendering obligations of governmental entities and private entities regarding public service projects and competitive business operations.

The SbD concept has gained ground and has been applied in engineering in recent years. In SbD, emphasis is put on responsible research and innovation, with a focus on safety and security about other important values such as well-being, sustainability, equality, and affordability [1–4]. SbD envisages an intellectual platform where the social sciences and humanities work together for technological development and innovation by helping to proactively incorporate safety considerations into engineering practices, while navigating between the extremes of technological optimism and excessive caution. In this way, SbD is also a practical tool for policy makers and risk assessors in designing management structures to encourage and meet safety and security requirements, while simultaneously acknowledging uncertainty [1]. It is challenging to find ways to reduce uncertainties that accompany modern systems with the complex interactions and emergent behavior that are inherent in present-day socio-technical systems. Dealing with uncertain risks requires measures different from those used in traditional risk assessment. For the risk management process to capture this, it should involve the co-evolution of knowledge, especially when risk data prove insufficient in the early stages of development. The concept of SbD enables this by engaging different stakeholders throughout the development process [2]. The expectations of different stakeholders towards SbD are not aligned. One way to resolve this issue is to make the viewpoints and expectations of others understandable and transparent to each other. For this to happen, communication between stakeholder groups must be enabled. It is essential to realize the importance of the design process in determining the level of safety and security during the use of a system or product. In such a process, it is necessary to ensure that the designer has a coherent and systematic way of considering possible safety and security problems and how to avoid them [3]. It is also argued that rather than directly designing for safety and security, it would be better to design with regard to responsibility for safety and security. Therefore, designers should also analyze where the responsibility for safety and security is best situated and design systems and technology accordingly [4].

The *Cambridge Dictionary* defines an actor as “a person or an organization that is involved in politics, society, etc. in some way because of their actions” (<https://dictionary.cambridge.org/dictionary/english/actor?q=Actor>, accessed on 16 December 2023). A stakeholder is also defined as “a person such as an employee, customer, or citizen who is involved with an organization, society, etc. and therefore has responsibilities towards it and an interest in its success” (<https://dictionary.cambridge.org/dictionary/english/stakeholder?q=Stakeholder>, accessed on 16 December 2023). In economic terms, this can be “an employee, investor, customer, etc. who is involved in or buys from a business and has an interest in its success”. Miles [5] discusses a stakeholder theory classification and recalls an early but comprehensive definition of a stakeholder, based on a dependency from which stakeholder power is derived. It states that actors may, e.g., provide essential raw materials, may control key marketing channels or resources, or may possess control over the organization’s financial well-being. Because the organization is dependent on the actors for their cooperation, the actors can influence the actions of the firm. It is also

argued that an actor cannot be a stakeholder without being in an actual relationship with the organization.

In the case analyzed here, the system is a major national infrastructure that concerns the interests of all citizens of Iceland. According to law, the country's local authorities (municipalities) are responsible for waste management, both for homes (individuals) and companies. According to law, these parties are responsible for sorting waste and must pay for the waste management service. According to the definition of actors and stakeholders, all citizens of Iceland are both actors and stakeholders in the system analyzed in this study.

Stakeholders can, furthermore, be viewed as both internal and external according to the nature of their relationships with the system [6,7]. Internal stakeholders help with organizational efficiency through production decisions. In contrast, external stakeholders help in aiding the organizational effectiveness through participative decision making, which involves an evaluation of the organization's legitimacy and the supply of resources to the organization [8]. Internal stakeholders include parties who are internal to the system or logically connected, e.g., employees, internal parties, and functional divisions of the system. External stakeholders include, e.g., regulators, competitors, and parties not logically connected. Since the system analyzed in this article does not yet exist, the decisions regarding stakeholders are only possible based on laws and regulations. In the beginning, the only internal stakeholders will be local authorities that already have legal responsibility. When decisions about the system are made, it will become clear who is directly involved in the project and will, thus, become an internal stakeholder. Others, e.g., regulators, will remain external stakeholders. Still other parties, e.g., the public administration, including the police, the judicial system, and the Directorate of Labor in Iceland, will certainly be actors, but will not have a direct interest in the system and are, therefore, not considered stakeholders in this analysis.

This study is based on a feasibility study conducted on a WtE project and published in December 2021 [9]. A group of experts within academia and industry worked together on the study to find a future solution for the treatment of combustible waste instead of landfills in Iceland. The feasibility study also included a pre-risk analysis with three different risks and hazards analysis techniques. One of those techniques is the systems theory (<https://www.sciencedirect.com/topics/psychology/systems-theory>, accessed on 12 November 2023) method Systems-Theoretic Process Analysis, STPA [10,11]. STPA is based on Systems-Theoretic Accident Model and Processes, STAMP, which is a causality accident modeling technique for identifying system hazards and safety-related constraints necessary to ensure acceptable risk in complex systems [10–12]. Given that a STAMP system model exists, STPA can be used to generate detailed safety requirements to prevent the occurrence of the identified hazardous scenarios. It is a top-down process addressing system components interactions and hazards/threats such as design errors and component interaction failures. STPA can be used for any system property, including cybersecurity. Due to limitations of the feasibility study, i.e., a short time frame, a vague system model, and a lack of knowledge about stakeholders and their relations and responsibilities, it was not possible to complete the analysis at the time.

With increasing demand for sustainability, transparency, and environmental protection, the scope of management and the responsibilities of managers are also growing. Management systems are often based on ISO standards like ISO 9001 for quality management systems [13], ISO 14001 for environmental management systems [14], ISO 27001 for information security management systems [15], and ISO 45001 for management systems of occupational health and safety [16], and previous research shows the growing importance of risk management in such systems and standards [17]. Recent articles also show the importance of accredited certification of management systems and businesses in "green" projects (https://www.researchgate.net/publication/301123031_Green_Project_Requirements_and_Strategies, accessed on 12 November 2023) like the one studied in this article [18–20].

Another study [21] shows evidence of flaws and risk issues in ISO-certified risk management systems. The study also shows that not all risk factors have been identified with conventional methods. Inconsistencies in risk terminology and lack of guidance in the standards have caused uncertainty regarding the identification, analysis, and management of risk. Therefore, certain weaknesses and flaws in risk management are evident in practice. The study also shows that with STPA, risk factors have been identified that could not be identified with previous methods based on ISO/IEC standards.

The authors' motivation originated in verifying feasibility and identifying risk factors in an important WtE project concept that promotes sustainability and will become an important element in the circular economy of an entire nation if executed. All aspects of the project concept must be analyzed as well as possible, creating an understanding of risk factors, and contributing to the best possible decision making during the preparation, design, and construction phases. Compensating later for making poor decisions, including those affecting safety and security, can be very ineffective and costly, as illustrated in Figure 1.

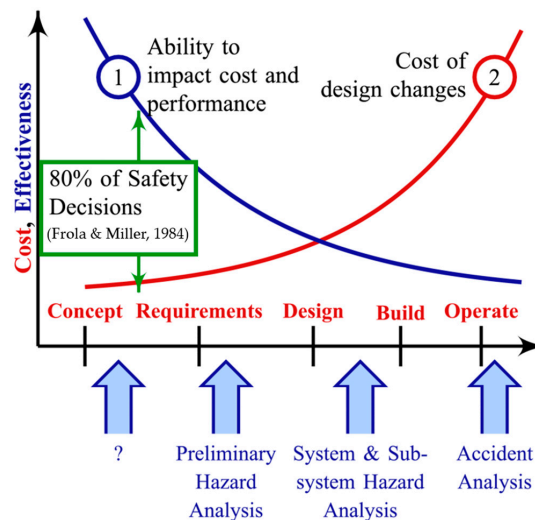


Figure 1. Decision effectiveness during life cycle [22,23]. © 2016 IEEE. Figure reprinted, with permission, from *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 12, pp. 3512–3523, Dec. 2016.

The authors' motivation for this study, furthermore, originated in decades of experience in applying ISO standards in ISO-certified management systems, as project managers, as directors, and as internal and external auditors. Experience has shown that identification and analysis of risk is an important but challenging factor in modern systems, not least during the preparation and design phases of projects and in the decision-making process. It provides the foundation for effective risk treatment, in decision making, design, development, production, construction, and operation. Conventional methods like Fault Tree Analysis and Failure Mode and Effects Analysis are not adequate for risk identification and analysis in complex socio-technical systems with many layers and interactions between individual system elements [11,22,24]. Such systems are non-linear, and time is an important factor, as is known from both systems theory (<https://www.sciencedirect.com/topics/psychology/systems-theory>, accessed on 12 November 2023) and control theory (<https://www.sciencedirect.com/topics/social-sciences/control-theory>, accessed on 12 November 2023). New methods and techniques are required to analyze risk in such systems. Therefore, the authors of this study want to investigate the efficacy of the relatively newly developed STAMP method and the derived analysis techniques, STPA and the Systems-Theoretic Early Concept Analysis, STECA [22,25,26], to analyze risk.

In this study, the authors have applied STAMP, STPA, and STECA techniques to develop a system model of a WtE project in Iceland and its implementation with the necessary control structure. The model is used to verify the WtE project concept and how best to start it and ensure that it succeeds. Furthermore, it can be used to conduct decision making from the beginning, taking risk into account. The aim of this study was:

1. To review the scientific literature on risk analysis conducted in recent WtE projects.
2. To review recent literature on the application of STAMP, STPA, and STECA.
3. To show how STAMP, STPA, and STECA can be applied to establish a system model that can then be used to confirm the concept, analyze the project risk, and define design requirements regarding risk in the early phases of the project.
4. To compare the results from this study to the results from risk analyses presented in recent articles on WtE projects; see the literature review in Section 3.

The novelty of this study lies in the combined application of STAMP, STPA, and STECA in a WtE project, a major national infrastructure project, and the detailed documentation of the process. To the knowledge of the authors, STAMP/STPA/STECA has not previously been applied to WtE projects, and the process has not yet been documented in the same detailed way. The article shows the implementation of STECA, but few articles have been published on the application of STECA.

This article is organized as follows. In Section 2, the context for the study is described; in Section 3, a literature review is conducted on both risk analysis in recent WtE and the application of STAMP/STPA/STECA; in Section 4, the research methodology is illustrated; in Section 5, the results are presented; in Section 6, a discussion on the results is given; and in Section 7, conclusions are drawn with thoughts on future work.

2. Context for the Study

This study is based on the results of a WtE feasibility study conducted in 2021, to prepare for the implementation of a future solution for the treatment of combustible waste for Iceland [9]. It contains expert analyses of the main factors concerning such a project. It reveals that exporting combustible waste is not a future solution and that preparations need to begin for the introduction of new methods and solutions for changing the treatment of waste generated in Iceland. The aim of this study is to take the project one step further and develop a system model that can be used for supporting the design and decision making in the project and, at the same time, to implement system safety and security into the project. This would be a megaproject on an Icelandic scale. (A megaproject is a very large-scale investment project. *The Oxford Handbook of Megaproject Management* gives a definition: “Megaprojects are large-scale, complex ventures that typically cost \$1 billion or more, take many years to develop and build, involve multiple public and private stakeholders, are transformational, and impact millions of people” [27]. Other sources have suggested that USD 1 billion is not a defining constraint; in some countries, a much smaller project (e.g., with a USD 100 million budget) could constitute a megaproject [28].) The waste disposal methods used in Iceland are listed in Table 1.

Table 1. Current and future waste disposal methods in Iceland.

Method	Definition	Description and Characteristics
Landfill	Waste collected in certain areas is compacted and wrapped in plastic. The bales are stacked in ditches and soil is layered over for natural decomposition and to improve appearance.	Landfills take up large areas of land and have a significant impact on the surrounding environment, both as a visible dumping ground and often, also, as an odorous pollutant as gas rises to the surface from decaying waste, where it is often hidden in mixed waste. Waste landfills are usually located near urban areas and cities to reduce transportation costs. Decomposition of landfilled waste is slow, and it takes waste more than 20 years to decompose in a cool climate like Iceland.

Table 1. Cont.

Method	Definition	Description and Characteristics
Compost	The biochemical effects of microorganisms are used to decompose and decay organic waste and turn it into fertilizer (manure).	Composting is the process of turning organic waste into compost. There are various methods of composting, but they have one thing in common: they create ideal conditions for the microbes that take care of the decomposition. During decomposition, the organic waste, e.g., the food scraps and garden waste, turns into nutritious compost that can be used to increase the fertility of the soil for cultivation and revegetation. During composting, the decomposition of the organic matter is accelerated by creating these ideal conditions for the microbes and insects that take care of the decomposition, but usually it happens quite slowly in nature.
Incineration	Waste is burned at high temperatures so that the waste materials are turned into ash, flue gases, and heat.	By incinerating waste, it is possible to get rid of combustible waste that would otherwise have to be landfilled. To ensure that the incineration is harmless, no toxic substances (e.g., batteries) or organic materials (e.g., animal carcasses or other organic waste) must be included with the waste to be incinerated. Otherwise, there is a risk of contamination, e.g., dioxin pollution.
WtE Incineration	WtE is a form of energy recovery that is not yet being used in Iceland but is now considered as a future waste treatment. It is the process of burning waste at high temperatures and, thus, generating energy in the form of electricity, heat, or fuel.	Most WtE processes generate electricity and/or heat directly through combustion or produce a combustible fuel commodity. All new WtE plants in OECD countries incinerating waste must meet strict emissions standards. Modern incineration plants are very different from older types of incineration plants, some of which have recovered neither energy nor materials. With the WtE incineration process, a harmless reduction of waste can be achieved, and the remaining material can be used in the construction industry and in road construction. The temperature of the combustion chamber exceeds 1000 °C and during combustion 95–96% of the original waste turns into very hot gas and ash [18]. WtE mainly leaves bottom ash and fly ash.

In the feasibility study, it is estimated that by 2030, up to 130,000 tons of combustible waste will be generated in Iceland per year. The production will generate 10 MW of electricity and 28 MW of heat (hot water). Ash and solid residues from the process can largely be used in road construction or as a building material. Although the energy will be sold, the operating costs will primarily be covered by charging gate fees. However, on average 70% of this capacity will be sufficient to run the incineration plant. Hazardous waste will not be accepted to ensure that solid residues from the plant are not contaminated. For comparison, the Amager Bakke WtE incineration plant in Denmark burns up to 400,000 tons of waste yearly (<https://www.power-technology.com/projects/amager-bakke-waste-energy-plant/>), accessed on 12 November 2023) (46 tons/h), and the Spittelau WtE plant in Austria burns around 250,000 tons yearly (<https://positionen.wienenergie.at/en/projects/spittelau-waste-incineration-plant/>) accessed on 12 November 2023) (29 tons/h).

WtE incineration plants that have recently been built around the world are often located close to densely populated areas, and no research has shown any harmful effects of their operation on human health or the ecosystem [29,30]. Environmental issues are a key factor in the preparation, design, construction, and operation of incineration plants. Important environmental factors are not only the possible pollution of air or water due to solid material flows, but also noise, odor, effects on health, ecosystems and vegetation, and visual effects. It is also necessary to look at possibilities for using energy and solid material streams. The intention is to carbon-offset all operations of the plant.

In the feasibility study, the choice of location has been examined from different perspectives, considering five sites identified in a report written on the need for waste incineration

plants in Iceland, prepared for the Icelandic Ministry of the Environment and Natural Resources in 2020 [31]. The choice of location must not only be based on transport cost, but also on opportunities for selling the energy, the positive attitude of the public, there being enough land for future development, and there being a reasonable distance from residential areas. Furthermore, there must be good access to labor, possibilities for carbon capture, and (important for Iceland) not a great risk of natural hazards like earthquakes and volcano eruptions, which are common in Iceland.

The feasibility study states that the capital expenditure (CAPEX) is expected to be 177.5 million EUR, including financial costs. There is an 80% probability that the final cost will be in the range of 135–236 million EUR. The explanation for this wide range in the cost estimate is that no design has yet been created. The project plan is primarily based on information from the COWI engineering consultant company in Denmark (<https://www.cowi.com/>, accessed on 12 November 2023), which has been involved in many similar projects in recent years. COWI has also made an estimate of the operational expenditure (OPEX), which is in the range of 57–80 EUR per ton with 35 full-time employees working at the plant. The profitability of the project was assessed by developing a financial model based on the CAPEX and OPEX, income from gate fees, and sale of energy, along with other assumptions. In the base case, it was assumed that a private company is established, that 80% of the CAPEX is borrowed at 8% interest rates, that the gate fee is 40 ISK/kg, and that the plant processes 100,000 tons annually. Based on these assumptions, the project is profitable, and the annual internal rate of return is about 12%. Sensitivity analysis shows that even if the CAPEX increases by 30%, the project is still profitable, and even if the OPEX increases by 50%, the project is still profitable. The feasibility is most sensitive to changes in gate fees and material quantity, and the project remains profitable while neither of these parameters is reduced by more than 15%. An estimate was made on how low the gate fee can be for the project to maintain profitability for two variations of ownership, where the interest rate is much lower than in the base case. In the case of a Public–Private Partnership (PPP) project, the gate fee must be higher than in the case of a purely public project.

There are different options regarding the types of organizations that could be formed around this waste incineration project. The decision, however, influences the extent to which the provisions of special legislation will apply to the operator, e.g., on whether waste incineration agreements may be exempt from tendering. To ensure this, the operator would have to be a public organization, but it is also possible that agreements with a private legal entity could be defined as internal agreements, and thus exempt from the obligation to tender. In the case of a PPP arrangement, the principles of competition law need to be carefully studied. A system could be set up to offset the transport costs of waste, especially if such a system has a better environmental impact and does not contribute to increased waste production. The rules of the EEA Agreement (<https://www.efta.int/eea/eea-agreement>, accessed on 12 November 2023) place restrictions on any kind of state aid intended to distort competition or favor companies. Such assistance is possible, provided that certain conditions are met. This could, for example, apply to an investment in energy production.

3. Literature Review

Section 3.1 reviews the scientific literature on risk analyses conducted in recent WtE incineration projects. Section 3.2 reviews the STAMP, STPA, and STECA literature, referring to techniques to identify hazards and threats that may lead to accidents, losses, and risks.

3.1. Scientific Literature on Risks and Risk Analyses in Recent WtE Projects

A search for published scientific articles on recent WtE projects on Google Scholar resulted in 16 articles and theses, which all were reviewed with regard to identification and analyses of risks. The articles all deal with high-tech WtE incineration plants and the importance of identifying risks in such projects. The literature shows that extensive, complex, and expensive infrastructure projects like WtE projects are often carried out as Public–Private Partnerships (PPPs). This is not only to finance the projects but also to

ensure access to the necessary knowledge for the project, to distribute risk, and to create a suitable framework for the project—all to ensure that the project is successfully executed. The WtE project analyzed in this study is similar to projects described in many scientific articles [29,30,32–43].

Risk assessment is important for PPP in WtE incineration projects, as described in [32], where a WtE project in China is investigated. Risk assessment promotes the sustainable development of WtE incineration plants. Some studies, however, do not consider the effects of the participation of many individuals and the resultant mutual compensation among risk factors. This affects the reliability of the evaluation of the results of the risk assessments and increases decision risk. The public sector commonly lacks knowledge and experience in PPP projects, and, particularly, risk allocation issues may prevent WtE incineration projects from succeeding [33]. It is possible to utilize a methodology based on weighted multiorganization fuzzy rough sets over two universes to perform risk evaluation for PPP in WtE incineration plant projects [32]. Although WtE projects are characterized by many advantages, such projects involve a variety of risk factors, e.g., economic risk, legal risk, political risk, environmental risk, social risk, and technical risk. These risk factors are usually created by many complex factors, e.g., large investments, long payback periods, government discretion, inadequate government oversight, and complex contractual relationships. All these factors have a major impact on all levels of the effectiveness of such projects.

A possible way to provide a framework for risk assessment for PPP in WtE projects is partly based on linguistic variables [34]. It is necessary to place emphasis on identifying risk factors that may accompany projects of this type throughout the life cycles of the projects. Uncertainty, which consists of fuzziness on the one hand and randomness on the other, is of great importance in risk assessment in an increasingly complex environment. The linguistic technique is used to express and explain unclear information (inaccurate wording of those involved in the assessment) and then, a calculation model is used to process the data. Most risk factors in PPP WtE incineration projects are generally assessed qualitatively rather than quantitatively and, therefore, it is important to carefully analyze the meaning of the words of the assessors, which can be very subjective. The main risk factors mentioned in [34] are: (1) public opposition, (2) lack of municipal waste, and (3) improper operation.

In recent years, it has been the policy of the Chinese government to develop waste incineration projects as PPP projects to achieve better and more efficient management of such projects [35]. Experience has revealed a variety of risk factors in such projects, which are associated with a lack of work experience and poor risk management. In [35], not only are the potential risk factors investigated, but also both the severity of risks and the likelihood of the realizations of risks are assessed. Views of experts in the field of waste industry were collected in a survey in the form of a questionnaire. Respondents were asked to evaluate a total of 18 risk factors that affect the success of PPP WTE projects, but these risk factors had previously been identified in former studies that were referenced. The results show that the risk factors that are considered most critical and to affect sustainability are: (1) public opposition, (2) governmental decision making, (3) shortcomings in the legal and regulatory system, (4) environmental pollution, (5) the lack of supporting infrastructure, (6) government credit.

In [36], critical risk factors in PPP WtE incineration projects are analyzed. Twenty-one risk factors are identified and analyzed, then ranked with regard to significance (1 = max, 21 = min): (1) public opposition, (2) environmental pollution, (3) land acquisition and administration approval risk, (4) revenue risk, (5) government credit risk, (6) governmental decision-making risk, (7) technical risk, (8) construction cost overruns, (9) operating cost overruns, (10) municipal solid waste supply risk, (11) incompleteness of laws or changes in laws, (12) private sector credit risk, (13) delays in completion, (14) design/construction/commissioning performance risk, (15) private sector decision-making risk, (16) operational performance risk, (17) unwillingness to pay, (18), interest rate risk, (19) force majeure, (20) inflation risk, (21) currency exchange risk.

Critical risk factors in WtE PPP in China are also discussed in [37]. The five most important risk factors in WtE PPP projects are identified based on an analysis drawn from real-life risk events in 14 such incinerator projects. These risk factors are (1) an inadequate waste supply, (2) unlicensed waste disposal, (3) environmental risk, (4) payment risk, and (5) a lack of infrastructure.

In [38], an interdisciplinary study was conducted on the criteria and accepted research framework (paradigm) for municipal solid waste management (MSW). The aim of the study was to identify influencing factors and present realistic indicators and measures for MSW from different perspectives. The study covers engineering, management, business, and social aspects. The study considers soil and underground pollution, air pollution, and the fight against global warming, which are complex and difficult issues.

A systematic review has been conducted of the literature on the health impacts of WtE emissions [29], notably the potential health effects (benefits and risk factors) of exposure from WtE projects. Little has been published regarding the health effects of such projects. In only 19 out of 269 articles surveyed, the health effects of WtE incinerators are addressed. Out of these 19 articles, 2 are on epidemiological studies, 5 on environmental monitoring, 7 on health effects, and 5 on life cycle assessment in such projects. The conclusion is that rigorous assessments (e.g., health impact or risk assessment, including sensitivity analyses) of WtE facilities and their technological characteristics and refuse type used are necessary when planning or proposing facilities to protect human health. Most life cycle assessment studies indicate that emissions from, and consequently health risks associated with, WtE plants are lower than those due to landfilling and conventional incineration. There is, however, an increased risk of lead pollution and pollution due to other heavy metals in sediment and fly ash that may be released into the environment at later stages of the life cycle. In this respect, proper design and operation of the WtE plants is required, as well as good management and monitoring of the emissions. Furthermore, continuous monitoring of environmental factors and health conditions is required to maximize both economic and environmental benefits, while minimizing harmful health effects and risks. Regarding the planning and design of WtE structures, it is important that a health risk assessment supported by comprehensive exposure monitoring and robust calculation models (e.g., accurate emission models, atmospheric models, and actual population data) is carried out before the proposed WtE incineration measures are implemented. It is important to ensure that measures work optimally. Also, careful consideration must be given to the health data used, the criteria used for the reference values, and the duration of the effects and their frequency. Sensitivity analysis needs to be performed to verify and test the criteria for health risk assessment and life expectancy assessment.

Environmental and health risks related to waste incineration are the subject of [30]. There, no research is found that strongly suggests that incinerators operating with modern technology and complying with emission laws carry an increased risk of cancer, infertility, or developmental disabilities. Proximity limits are not defined. There are three factors that support this:

1. Emissions from incinerators now being built in developed countries for waste incineration are much lower than before. The epidemiological studies that have been carried out that revealed negative effects on health relate to older types of such incinerators;
2. Risk assessment studies indicate that most of the exposure is through people's diets;
3. Dioxin level studies in residents living near incineration plants have not shown an increase in this level compared to residents living in reference areas.

However, studies exist showing that people who live and work near waste incineration plants believe they are exposed to various types of health damage. The mentioned effects include cancer, adverse effects on the respiratory system, heart disease, effects on the immune system, increased allergies, and malformations in children. Despite this, it has not been possible to link such illnesses and risk factors directly to pollution from high-tech waste incinerators.

Legislation regarding WtE plants is different between countries, including countries belonging to the EU. In [39], it is argued that favorable legislation has enabled Denmark to become a leader in the category of high-tech WtE incineration plants, whereas Italy is on the other end of the spectrum due to non-favorable legislation. The EU's environmental goals have, in the Nordic countries, facilitated investment in waste management and contributed to better and more environmentally friendly high-tech incinerators. Reducing greenhouse gases through improved waste management is one of the main policy challenges in the EU's environmental program. The Waste Framework Directive (EU Directive 2008/98/EC) classifies waste treatment as "energy recovery" rather than "disposal". With the EU Directive, WtE gained a role and weight in the circular economy. WtE incinerators now play an important role in protecting clean/non-toxic cycles and treating non-recyclable waste. The function of such plants is to clean/decontaminate waste streams and remove waste with toxic substances from the recycling ring. The WtE incinerators help keep the recycling economy clean by acting as a scrubber for pollutants. The only other treatment for this waste stream would be landfills, which is not advantageous.

Public communication is needed to build positive attitudes and acceptance regarding the construction and operation of high-tech incineration plants for waste [40]. People's opposition to WtE plants is mostly related to fear of negative effects on the environment, risks to the health or safety of the inhabitants, or a reduction in the status of the territory. Communication can not only contribute to the success of and consensus about incineration plants but can also play a key role in strengthening people's willingness to participate in the circular economy. Public debate on waste issues within European institutions and public opinion within European countries is characterized by differing views of the people of these countries. In many other areas, the public seems to lack understanding and is opposed to the construction of waste incineration plants. To mitigate the risk of public opposition, it is suggested that those responsible for WtE projects should develop a communication policy wherein the main stakeholders and participants in projects are made to disseminate information and knowledge to the public in an accessible way so that it is easy to understand.

A possible relationship between WtE plants and electric cars is depicted in [41]. Following the ideas, an urban microgrid consisting of a WtE combined heat and power generation unit and charging stations for plug-in electric vehicles could be devised. The main purpose is to provide additional services and speed up the introduction of electric cars.

Finding the optimal time to start a WtE incineration project is not obvious. The values of waiting vs. switching technologies from landfills to WtE systems must be evaluated. In [42], it is concluded that it is best to invest immediately in either incineration or gasification, as delaying investment results in a loss of opportunity for energy generation with WtE systems. At the same time, it is emphasized that the government must support the WtE program as it will make a significant contribution to solving problems in the environment, especially regarding air quality and waste management as well as energy security and sustainability.

Investment risk in WtE projects is considerable and needs to be assessed [43]. One approach is to estimate future competition in the waste market by building complex simulation models. This may be approached by defining a waste availability factor for use in the assessment. Since the presence of a sufficient supply of waste is one of the major risk factors in WtE projects, its evaluation represents an important part of feasibility studies for such projects.

The construction of a high-tech incineration plant in Amager Bakke in Copenhagen, Denmark is described in [44]. The innovative steel structure of the plant and its roof, which is designed as an outdoor recreation area for the public, are described. Construction of the plant began in 2013 and its operation started in 2016 (officially opened in March 2017). The incineration plant is 43,000 m² and the roof of the building rises to a height of 85 m. The roof is a garden the size of two and a half soccer fields with trees. It offers areas for hiking, climbing, and skiing, a viewing platform, and a café. However, a special law deals

with the risk regarding the design of the plant's chimney, which does not rest on its own foundation (ground support) but is connected to the steel structure of the main building at a height of about 20 m and, therefore, appears to hang visually on the outside of the building. The location of the chimney on the gable of the main building and the rather weak foundation causes the risk of excessive vibration due to wind, which had to be considered when designing the plant.

Though the WtE plant at Amager Bakke has been in operation for only a few years, there is already a demand for change that requires impact analysis and environmental assessment [45]. Although the plant is one of the most advanced in the world, there is reason to update the technology and add carbon capture and storage (CCS) to reduce the environmental impact of the waste incineration. In [45], a detailed analysis is made of the impact of changing the plant's incinerator at Amager Bakke (capacity: 600,000 tons of waste per year) using CCS as a post-incineration technology.

What the scientific articles in this section state about risk in WtE projects can be summarized as follows:

1. Risk is associated with big and complex projects (i.e., megaprojects) that take several years. Circumstances can change over time and various project criteria can change [29,32–38];
2. Establishing WtE projects as PPP projects is one way to mitigate project risk, for example, financial risk [32–37];
3. People's fear of environmental pollution causes public opposition and a bad image of waste incinerators. This creates risk and complicates WtE projects [30,35,40];
4. There is a risk due to inadequate communication and lack of communication with the public [40];
5. National legislation regarding WtE involves risk. Risk is associated with inconsistencies and unclear legal provisions. Governmental decision making and shortcomings in legal and regulatory systems are risk factors [32,35,39];
6. Project financing is a risk factor and state backing is important [34,35];
7. Unclear risk allocation in PPP projects creates risk [33];
8. All decision making in WtE projects must be based on results from risk analysis and risk assessment, i.e., planning, design, implementation, and operation of WtE incineration plants [33];
9. In WtE projects, it is common for communities to develop their "own" risk analysis methods that take into account the local environment, situation, and culture [33];
10. Criteria used in risk analysis need to be carefully considered, and they need to be kept under continual review [29,30];
11. The effects on the health of people working or living in the vicinity of WtE incineration plants have not been sufficiently studied. Long-term and life cycle research needs to be done. Continuous monitoring and review of standards is important in all existing high-tech incineration plants [29];
12. The deposition of energy and heat from WtE plants influences site selection [41];
13. The choice of the location and appearance of buildings is important to the public. A positive image of a high-tech incinerator can support a circular economy, improve the public's environmental awareness, and strengthen the willingness of people to take an active part in any kind of sustainability project [40,44];
14. Technology is ever-evolving. It can be assumed that the equipment of high-tech incinerators needs to be renewed regularly [45];
15. Delaying investment results in a loss of opportunity for selling the products from the WtE plant [42];
16. There is no mention of ISO standards or their use in the scientific articles, neither ISO management system standards (<https://www.iso.org/management-system-standards.html>, accessed on 12 November 2023) nor ISO risk management guidelines like ISO 31000 [46], which is the guiding standard for risk management referenced in all ISO management standards.

3.2. Literature Review on STAMP, STPA, and STECA

Systems-Theoretic Accident Model and Processes (STAMP) is a causality accident modeling technique for identifying system hazards and safety-related constraints necessary to ensure acceptable risk in complex systems [10–12]. STAMP is a recent technique, first developed by Leveson in 2004 [10] but since then widely applied and tested in many fields.

Systems-Theoretic Process Analysis (STPA) is a hazard/threat analysis technique, derived from STAMP and based on systems theory (<https://www.sciencedirect.com/topics/psychology/systems-theory>, accessed on 12 November 2023). Since being introduced [11], STPA has been developed further to also analyze the security of systems with STPA-Sec [39], and Systems-Theoretic Early Concept Analysis with STECA [22,25,26]. Scientific studies have been conducted on the use of STPA in many areas, e.g., aviation, spacecraft, healthcare, railroads, automobiles, military, nuclear power plants, oil, gas (petrochemicals), and energy. Interdisciplinary studies have also been conducted on, e.g., human factors and safety, integration of safety into systems engineering processes, identifying leading indicators of increasing risk, application of standards and certification, and the roles of cultural, social, and legal systems in safety and security. To the knowledge of the authors, STAMP/STPA has not been applied in WtE projects and no scientific articles or reports on STAMP/STPA in such projects were found on Google Scholar.

According to the STPA handbook [47], basic STPA is conducted in four main steps:

1. Define the purpose of the analysis;
2. Model the control structure in accordance with STAMP;
3. Identify unsafe control actions;
4. Identify loss scenarios.

Figure 2 gives an overview of the STPA iterative analysis process as described in [47]. STPA is still being developed as a technique in many parts of the world, especially steps 3 and 4. This is described in many recent scientific articles, either as a theoretical analysis of the technique or as case study articles on actual application examples. In this review, the focus is on the practical application of the STAMP/STPA technique in an early-stage project concept. Therefore, STECA, as an early concept analysis variant of STAMP/STPA, is an interesting technique to test and confirm the feasibility of the WtE project. In STECA, the emphasis is on preparing a model to be used for safety/security hazard analysis during the preliminary inspection of the project. Since the WtE project is only at the discussion stage and no decisions have been made of any kind, it is neither possible to make scenarios about “unsafe control actions” nor to “identify loss scenarios”. It is only possible to take the first two STPA steps out of the four, i.e., to define the scope and develop the model.

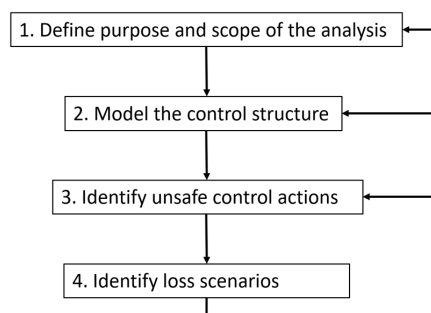


Figure 2. An overview of the STPA iterative analysis process, in four steps.

STECA consists of two basic steps. The first step involves recursively applying control-theoretic concepts using guide words, heuristics, and feedback control criteria to parse the existing concept report and review it with regard to statutory and regulatory requirements [22,48]. Also, the main results regarding the project, e.g., the waste amount

and possible location, are used as Concepts of Operations (ConOps), resulting in the development of a control structure of the model of the concept. With STECA, it should be possible to determine the hierarchical control structure but, in this case, it is not relevant since laws and regulations determine the hierarchical structure for the most part. The second step in STECA, the analysis, consists of examining the resulting model with the explicit goal of identifying hazardous/threat scenarios, information gaps, inconsistencies, and potential tradeoffs and alternatives. The analysis aims at identifying incompleteness or gaps in the control structure, ensuring that all safety/security-related responsibilities are accounted for, and identifying sources of uncoordinated or inconsistent control [22,25], that is, to perform the following functions:

1. Identify incompleteness or gaps in the control structure;
2. Ensure that all safety-related responsibilities are accounted for;
3. Identify sources of uncoordinated or inconsistent control.

Figure 3 shows a simple but typical STPA control loop [22].

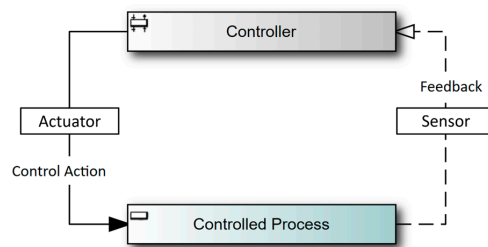


Figure 3. A simple STPA control loop.

This section reviews articles on the application of STAMP, STPA, and STECA. Such articles have been written in various fields, although not about WtE according to the knowledge of the authors of this article.

In the first article, Chaal et al. [49] propose a framework to support the model development, or hierarchical control structure, of an autonomous vessel. They use STAMP, STPA, and STECA as the foundation of the proposed framework. STECA is applied to verify the control structure for completeness, safety-related responsibilities, coordination, and consistency. The framework utilizes the current shipping operation system, the available information about autonomous vessels, and seafarers' experiences on board conventional ships. The authors refer to the STPA handbook and point out that the guidance does not always provide the necessary level of support when developing a control structure of a new design. The level of knowledge required is different for every new design, which means that a different starting point is needed for the development of each new system. The framework proposed in this case is a supporting tool for using the available knowledge about the concept of an autonomous vessel and the knowledge about traditional vessel operations to define a control structure of an autonomous vessel. It provides additional support for applying STPA in the design phases of autonomous vessels.

Sultana et al. [50] evaluate the feasibility of using STPA in process industry applications. High levels of automation and complex system interactions in the process industry have brought new challenges to risk management. Traditional hazard analysis techniques (such as a hazard and operability study, HAZOP) are not sufficient to analyze risk. Sultana et al. compare STPA and a HAZOP to determine whether STPA can replace traditional HAZOPs when transferring liquefied natural gas from one ship to another. Their results show that STPA is complementary to traditional HAZOPs.

Friedberg et al. [51] analyze safety and security risk in a smart grid, a complex cyber-physical system. The authors apply STPA as an integrated STPA-SafeSec approach to analyze both safety and security aspects together in a single framework. Their results show that safety and security need to be analyzed together to identify a full set of system loss

scenarios. The results, furthermore, show that STPA-SafeSec does not directly provide quantifiable results. Friedberg et al., however, point out that by combining STPA with traditional techniques like HAZOPs, more quantifiable results may be obtained.

Dakwat and Villani [52] present a method for combining STPA and system model checking with a technique called UPPAAL (<https://uppaal.org/>, accessed on 12 November 2023) (developed in collaboration between Uppsala University in Sweden and Aalborg University in Denmark) during product development, in order to provide a formal and unambiguous representation of the system being analyzed. They conducted a practical case study of a robotic flight simulator as an example of the proposed method. The result indicates that by merging the two techniques, system knowledge can be improved. STPA is used to analyze control actions and identify safety constraints, and then update and verify the system model.

Bjerga et al. [53] address uncertainty treatment in the risk analysis of complex systems. They name STPA and the Functional Resonance Analysis Method (FRAM) as examples of suitable approaches to analyze risk in such systems. Their focus is on the treatment of uncertainty and potential surprises linked to the operation of complex systems. They warn against abandoning probability as the consequence can be that important aspects of risk and uncertainty are ignored, which leads to poor decision making. Bjerga et al. contrast two views on how to proceed in the case of an uncertain/inadequate probability model: (a) reduce uncertainty by better modeling of the system; (b) characterize uncertainty better. They argue that both are needed.

Jamot and Park [54] present a case study where STAMP/STPA is applied for risk assessment in a real construction project. The study was carried out to check the applicability of the STPA technique where Probabilistic Risk Analysis (PRA) had initially been used by the project team. After going through a risk analysis on the project with STPA, five members of the project team were asked to evaluate in a questionnaire (on scale 0 = poor to 5 = excellent) their experience working with STPA compared to using PRA. The STPA technique received a good rating of 3.6 for risk identification, 3.4 for risk mitigation, and 3.2 for its structure. On the other hand, the average rating was 2.6 for the analysis time, and 2.4 for the complexity of the method. It is unclear from the paper whether the project members evaluating the STPA technique had more previous experience with the PRA technique and what effect this may have had. The authors, however, conclude that for dealing with complex construction projects, the STPA approach seems to deliver higher-quality results compared to the PRA approach since its main objective is to simulate possible scenarios.

Sulaman et al. [55] present a comparative study where STPA and Failure Mode and Effect Analysis (FMEA) are both used to analyze the same forward collision avoidance system. These techniques have different focuses, and STPA is a top-down analysis technique, whereas FMEA is a bottom-up analysis technique. FMEA especially takes the architecture and complexity of components into account, whereas STPA is stronger in finding causal factors of identified hazards. The comparison in the study shows that FMEA and STPA deliver similar results.

The lessons learned from the above articles on STAMP, STPA, and STECA can be summarized:

1. The STAMP, STPA, and STECA techniques are helpful in developing new and complex systems;
2. The STAMP and STECA techniques are helpful in early concept analysis and building system models;
3. The STAMP and STPA techniques are helpful in further design, especially when analyzing complex systems and projects;
4. The STPA handbook does not always provide the necessary guidance and level of support when developing a control structure of a new system;
5. STAMP and STPA are often complementary to other analysis techniques, e.g., HAZOP, UPPAAL, FRAM, FMEA.

4. Research Methodology

In this study, the systems theory-based STAMP method was applied together with the derived hazard/threat analysis techniques STPA and STECA. A system model was created with STAMP showing stakeholders and their communication. The first steps of STPA were taken by identifying major losses/accidents and system-level hazards/threats that can lead to losses/accidents. To be able to conduct a full STPA, the system must, however, be defined and known. There, STECA is useful as a technique/tool to analyze the necessary system elements and the corresponding communication, in terms of both actions and feedback. In this case, STECA together with STPA was used to help define the WtE project scope and to clarify who the stakeholders must be, their responsibilities, and their connection and necessary communication with each other. This was done to identify the prime risk factors in the first phase of the project. This research proceeded in the following ten steps:

1. Definition of the scope of the WtE project;
2. Review of all relevant Icelandic laws and regulations on waste management, environmental issues, local government issues, health issues, building regulations, and the European directives on environmental issues in relation to roles and responsibilities in a WtE project;
3. Definition of stakeholders, based on step 1 and 2;
4. Definition of roles and responsibilities of all stakeholders from step 3 based on requirements in laws and regulations reviewed in step 2;
5. Creation of a first draft of the control structure of the WtE system, representing stakeholders and their communication, based on the stakeholder analysis in steps 3 and 4. A graph was made of the communication required between stakeholders according to laws and regulations, in terms of both feedback and control actions, resulting from step 4;
6. Identification of control actions as subsystems where there might be a reason to make special models;
7. Review of a STAMP system model by stakeholders and actors in different fields. Validation was sought for every part of the STAMP system model, i.e., stakeholders, responsibilities, feedback needed, control actions needed, and sub-processes within the model. See Appendices A–C;
8. The first two steps were taken in STPA based on the validated STAMP system model. Stakeholders and actors, experts on individual project aspects from step 7, were asked which losses/accidents and system-level hazards/threats may not occur in the project at all, and furthermore, which hazards/threats they believed could cause such losses/accidents. These two STPA steps further confirmed the STAMP model and pointed to important aspects of the project discussed in the results section;
9. Review of the project scope;
10. Refinement of the STAMP system model, and description of control actions made. Control action analysis was performed regarding whether an action is (a) a requirement, (b) an output, (c) a one-time action, or (d) a continuous action.

In this case study, the STECA process was followed as shown in Figure 4 [56].

The STAMP model for the WtE project was iterated and individual factors were verified in various ways for model integrity and analyzed as described in Section 6.

If the STECA process is followed further, then the analysis continues with the modeling and analyses of the hierarchical safety/security control structure. In this study, hierarchical control is not critical. It is, at this point, defined by laws and regulations. The modeling analysis is focused on (a) the identification of stakeholders, (b) the responsibilities of stakeholders, (b) feedback needed from stakeholders, (c) actions required from stakeholders, and (d) descriptions of actions. Table 2 shows the control-theoretic analysis of textual or graphical information from the feasibility study and from document review.

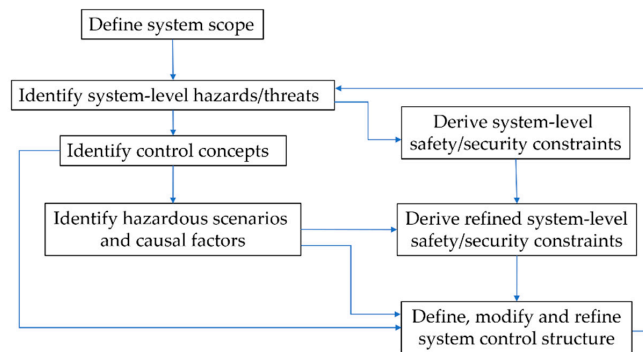


Figure 4. The STECA methodology.

Table 2. Control-theoretic analysis of textual or graphical information, based on STECA.

Name of Model Item/Element	Definition
Stakeholder (matches “source/subject” in STECA)	A legal entity that is required in the project.
Responsibility (matches “role” in STECA)	Legal responsibility as stated in law or role necessary for some reason, which should be documented.
Feedback needed (from which stakeholder(s)? (matches “behavior type” of the nature “action” in STECA)	For a given responsibility/role, which type(s) of feedback behavior are required or exhibited?
Action required (towards which stakeholder(s)? (matches “behavior type” of the nature “action” in STECA)	Description of control action (CA): (a) is it a clear control action, (b) is it a requirement, (c) is it a simple output?

No further STPA steps can be taken at this point. For that to happen, a decision must be made on several important factors, e.g., who will participate in the project and the project ownership setup (owner structure), what location will be chosen for the incineration plant, and what is the time frame of the project, i.e., when should the project start and when should it end? Time is a sensitive factor due to political risks and the local and parliament elections being held every four years.

There are few software tools that can support risk analysis with STAMP/STPA/STECA. The software tool (<https://www.riskmanagementstudio.com/stpa-software-solution/>, accessed on 12 November 2023) used in the study for modeling is the product of a collaboration between Stiki (<https://www.stiki.eu/en/> accessed on 12 November 2023) in Iceland and The Zurich University of Applied Sciences (<https://www.zhaw.ch/en/university/> accessed on 12 November 2023) in Switzerland, a product of a Eurostars project funded for three years [57,58].

5. The Results

A simplified STAMP system model of the WtE project with a generic control loop is shown in Figure 5. The controlled process is the WtE project, and the controller is the management of the whole project.

Having only this simplified control structure, the expert team from the WtE feasibility study [9] was guided through the first step in the STPA, shown in Figure 2, by asking two questions. This first STPA step is divided into four parts: (1) identify losses, (2) identify system-level hazards/threats, (3) identify system-level constraints, (4) refine hazards/threats (optional). So, having assumed that the decision to build a WtE plant in Iceland had been made, the questions asked are listed below. (See a list of those who were asked in Appendix A and examples of the questions and answers in Appendix B).

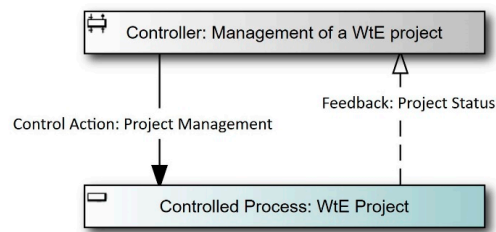


Figure 5. A generic control loop of a WtE project.

1. What types of losses/accidents does the analysis aim to prevent—What major loss/accident should not happen during the design and construction period? (Name 1–3);
2. What system-level hazard/threat could result in such a loss? (Name 1–3 for each loss/accident).

Table 3 shows the answers received, sorted by frequency. Three major losses were identified and the one considered most serious was “The project stops before it finishes”.

Table 3. Losses/accidents that should be prevented in the WtE project.

Loss Id	Name of Loss
L-1	The project stops before it finishes
L-2	Serious accidents to people
L-3	Delays in completing the project

Table 4 presents the answers received when asked about system-level hazards/threats that could result in a loss. The answers were not all descriptions of system-level hazards/threats at this point.

Table 4. Hazards/threats that might result in loss—answers received.

Hazard/Threat Id	Name of a Hazard/Threat	Resulting Losses
H-1	It is not possible to finance the preliminary project	L-1, L-3
H-2	Disputes arise between parties that are not covered by contracts and cannot be resolved	L-1, L-3
H-3	Design criteria change during the project time	L-1, L-3
H-4	Costs exceed budget	L-1, L-3
H-5	Time and progress plan fail, e.g., due to strikes or delays in construction permits	L-1, L-3
H-6	Opposition to the project, a negative image	L-1
H-7	Business plan fails	L-1, L-3
H-8	Waste plan fails	L-1
H-9	Inadequate project management	L-1, L-2, L-3
H-10	Lack of safety culture and accident prevention	L-2, L-3
H-11	Allocation/splitting of risk is unclear	L-2, L-3

The system-level hazards/threats derived from the answers in Table 4 are shown in Table 5. The refined system-level hazards/threats are presented with the responsive system-level constraints (SLH-1 = H-1 + H-4, SHL-2 = H-2 + H-11, SLH-4 = H-4 + H-7 + H-8).

Table 5. System-level hazards/threats (refined) and constraints.

System-Level Hazard/Threat and Constraint	System-Level Hazard/Threat System Level Constraint	Resulting Losses
SLH-1 SLC-1	<ul style="list-style-type: none"> Project is not fully financed. Project must be fully financed. 	L-1, L-3
SLH-2 SLC-2	<ul style="list-style-type: none"> Project contracts are not clear so that unresolvable disputes arise between parties. Project contracts between parties must be clear so that unresolvable disputes will not arise between parties. 	L-1, L-3
SLH-3 SLC-3	<ul style="list-style-type: none"> Project design criteria change during the project time. Project design criteria must be validated and confirmed during the project time. 	L-1, L-3
SLH-4 SLC-4	<ul style="list-style-type: none"> Project business plans (time, cost) fail. Project business plans (time, cost) must be reliable and must not fail. 	L-1, L-3
SLH-5 SLC-5	<ul style="list-style-type: none"> Project experiences opposition and a negative image from the public. Project must enjoy a positive attitude/image in the public during the project period. 	L-1
SLH-6 SLC-6	<ul style="list-style-type: none"> Project management is inadequate during the project time. Project management must be maintained during the project time. 	L-1, L-2, L-3
SLH-7 SLC-7	<ul style="list-style-type: none"> Project safety culture is not maintained. Project safety culture must be maintained during the project. 	L-2, L-3

When it comes to modeling the system control structure, a review of Icelandic laws and regulations reveals which main stakeholders would be involved in the preparation and construction phase of the WtE project. Some of them serve the same purpose and are, therefore, grouped together as a single entity, e.g., the municipalities are grouped in S-1 and the licensors in S10. This makes a total of 26 stakeholders that are listed in Table 6.

Table 6. List of stakeholders in the WtE project and their roles and responsibilities in the preparation and construction phase.

Stakeholder Id	Names of Stakeholders in the Construction Phase	Roles and Responsibilities of Stakeholders
S-1	Municipalities	<ul style="list-style-type: none"> • Legal obligation to dispose of waste in a sustainable way • Responsibility for establishing the proper governance in the preparation and early decision-making phase of the project • Project feasibility study • Project risk assessment • Responsibility for financing the whole project • Establishing the PPP for the project • Supervisor role
S-2	Waste Municipal Association (WMA)	<ul style="list-style-type: none"> • Serves the municipalities in establishing the WtE project • Knowledge source
S-3	WtE Ltd.—project owner	<ul style="list-style-type: none"> • Project owner (PPP affiliate) • Project mgmt., incl. quality, health and safety, environmental and sustainability requirements • Ensures project financing • Daily supervision during project time • Appoints a design manager • Appoints a construction manager • Assigns auditors • Applies for a construction permit for the intended project and provides the necessary data, e.g., environmental assessment
S-4	Ministry of the Environment, Energy and Climate	<ul style="list-style-type: none"> • Waste matters in accordance with the provisions of the regulatory framework for waste management, i.a., obligations under EEA law
S-5	The Environment Agency of Iceland	<ul style="list-style-type: none"> • Enforces laws on pollution prevention, environmental responsibility, nature conservation, and hygiene—sets environmental regulation • Issuance of operating license for the WtE plant
S-6	Municipality port	<ul style="list-style-type: none"> • Provides harbor facilities for shipping to and from WtE plant location • Examines conditions for harbor construction
S-7	National Planning Agency	<ul style="list-style-type: none"> • Implementation of laws and regulations on environmental assessment of projects and plans • Presents the project owner's assessment plans and environmental assessment reports • Issues an opinion on assessment plans and on the environmental assessment of a project based on the developer's environmental assessment report and comments received on it
S-8	The Road and Coastal Administration	<ul style="list-style-type: none"> • Determines the roadway • Negotiates with landowners • Road design

Table 6. Cont.

Stakeholder Id	Names of Stakeholders in the Construction Phase	Roles and Responsibilities of Stakeholders
S-9	Regulatory body for buildings and constructions	<ul style="list-style-type: none"> Monitoring of the implementation and compliance with laws and regulations reg. building and construction Investigation of whether building regulations are violated or not followed Operation of a database for information on buildings and construction
S-10	Building licensor (municipality/landowner) of WtE construction site (many sub-institutions, fire brigade, health committee, planning committee, and politicians)	<ul style="list-style-type: none"> Review of building permit application and building documents Confirming consistency in the regional development plans Granting a building permit Investigation of major accidents and injuries Work status checks
S-11	Parliament	<ul style="list-style-type: none"> Makes legislation reg. waste disposal, environment, health and safety
S-12	European Union (EU)	<ul style="list-style-type: none"> Coordinates waste and environmental issues within the EU Working groups with the participation of individual countries
S-13	Investors	<ul style="list-style-type: none"> Co-finance
S-14	Banks	<ul style="list-style-type: none"> Co-finance
S-15	Main contractor	<ul style="list-style-type: none"> Human resources available when needed Necessary equipment available when needed Project management on site Tendering and selection of subcontractors Project risk assessment Coordination of subcontractors Assesses, monitors, and manages risk on project site Finishes the project on time
S-16	Subcontractors	<ul style="list-style-type: none"> Subcontractors available on time Risk assessment for work packages carried out Professional knowledge and experience
S-17	Design manager	<ul style="list-style-type: none"> Submission of design data/drawings for approval for a building permit application Compiles a report on the designer's area of responsibility and confirms with their signature that it is a comprehensive overview Handles the owner's internal control for the design of the construction Organization of coordination of design data

Table 6. Cont.

Stakeholder Id	Names of Stakeholders in the Construction Phase	Roles and Responsibilities of Stakeholders
S-18	Construction manager	<ul style="list-style-type: none"> • Makes written agreement with the master craftspeople which they hire on behalf of the owner • Carries out the owner's internal control from the time the building permit is issued until the final assessment has taken place • Carries out phased audits according to the inspection manuals • Professional representative of the project owner [S-3] • Requests a final audit before the WtE plant is started • Operation of a quality management system
S-19	Engineers, consultants, and designers	<ul style="list-style-type: none"> • Business plan • Risk analysis and risk assessment • Information gathering • Design of the WtE plant
S-20	Insurance companies	<ul style="list-style-type: none"> • Insurance
S-21	Auditors, inspection agencies, e.g., the Government Property Agency	<ul style="list-style-type: none"> • Auditing standards and process • Financial auditing • Health and safety, quality, security, and environmental management auditing • ESG auditing
S-22	The public	<ul style="list-style-type: none"> • Approve of the project • Remain critically engaged
S-23	Parties of the labor market	<ul style="list-style-type: none"> • Preserve peace in the labor market
S-24	Electrical grid company	<ul style="list-style-type: none"> • Provides a connection to an electricity transmission system through a substation • Transmits electrical power generated by the WtE plant to buyers
S-25	Hot water distribution company	<ul style="list-style-type: none"> • Provides a connection to the hot water distribution system • Distributes the hot water coming from the WtE plant
S-26	Concrete plants and tarmac production units (buildings and roads)	<ul style="list-style-type: none"> • Use of good and affordable additive building materials

The STAMP system model with its control structure of the WtE project is shown in Figure 6. The actual project, the construction of the WtE incineration plant, is the controlled process and is shown with the red color in the bottom half of the figure. The model is not presented in a hierarchical form, but is organized with regard to time factors in the project, with early involvement shown from the top and later involvement towards the bottom. The figure shows 26 stakeholders (listed in Table 6) displayed as gray-colored controllers and one red-colored controlled process. Figure 6 shows a simplified interaction that consists of necessary feedback and control actions occurring between stakeholders.

Figure 6 shows that the project owner plays a central role in the system and the project. Until the project owner group has been established, the Waste Municipality Association (WMA), stakeholder S-2, functions as a think tank and drives the project forward—it is already responsible for processing more than half of all waste in Iceland. Six municipalities in the capital area of Iceland, representing 63% of Iceland’s population (<https://static.is/publications/news-archive/inhabitants/the-population-on-january-1st-2022/>, accessed on 12 November 2023), build the owner group of the WMA. They are marked as stakeholder S-1 in the STAMP model. They play a leading role in the preparation phase of the project, together with S-2. The business is controlled by politically elected representatives, with authority only for four years at a time (<https://ssh.is/english>, accessed on 12 November 2023). These two stakeholders do not have the financial resources to execute this project alone. Therefore, a partnership of public and private investors is needed. A review of current laws on waste management and the responsibilities and duties of municipalities reveals uncertainties in many aspects of this kind of project.

The STAMP system model shows the feedback every stakeholder needs to give, with broken arrow lines, in order to fulfill their roles and responsibilities. In the same way, the control action required from each stakeholder is shown with an unbroken arrow line. For the project to be interesting to investors, the flow of material for incineration must be guaranteed. In most countries, the products of the incineration plant will be in demand for energy buyers, both electricity and hot water. In Iceland, however, there is already enough of a supply of both electricity and hot water at a relatively low price. The motivation is, therefore, primarily for the country to be sustainable regarding waste management and independent from other countries. This makes it a more challenging business plan. Stakeholders S-13 and S-14 are needed to finance the project, but they need assurance for their investment. The municipalities also need assurance that the project will be completed, and that the incineration plant will be able to fulfill their duties regarding waste management. The next step in the modeling process is, therefore, to focus on how this challenge can be met and to take a closer look at the project owner function, i.e., stakeholder S-3.

Iceland’s waste management is governed by Act No. 55/2003, which places an obligation on local authorities to operate reception and collection centers, sometimes referred to as disposal sites. This legislation also sets limits on the WMA (stakeholder S-2) disposal of household waste. Public procurement projects of governmental entities are subject to tender as per Act No. 84/2007, contingent on circumstances within the European Economic Area (EEA). Additionally, the activities of the WMA are governed by Act No. 44/2005 on competition, which prohibits the abuse of market-dominant and monopoly positions.

It is plausible to consider that the already existing WMA could serve as the proprietor of an incineration plant. This aligns with the legal mandate for municipalities to establish waste management channels. The rationale supporting an incineration plant mirrors that of the existing landfill’s operation. This holds true even if the incineration plant operates under a distinct WMA organization as an autonomous business unit, maintaining compliance with the same legal framework.

The existing WMA is equipped to oversee the incineration of all household waste, given municipalities’ obligation to collect and manage it. On the other hand, waste from businesses and industries is handled by private entities. Consequently, maintaining competitive gate fees becomes a crucial requirement. As the activity falls under the purview of Act no. 44/2005 on competition, careful steps must be taken when implementing measures to secure a steady supply of waste for the incineration plant.

Incineration of waste for the WMA (S-2) is subject to tender in the EEA (S-11 and S-12) unless the association takes care of it itself. An exemption from this is granted if the operator of the incineration plant is a public entity and if 80% of the plant’s projects are assigned to the plant by public entities.

The first steps taken here with the STAMP modeling of the WtE project, and preliminary risk analysis with STPA and STECA, highlight the assumptions that must be laid as a basis for a project like this. Based on the assumptions of the project stated here, the following five scenarios can be thought of as possible advantages for the WtE project owner in terms of structure or setup of the project:

1. Public ownership, implementation, and operation;
2. Public ownership, but private implementation/execution and operation;
3. Private ownership and implementation/execution, but public operation (property leased to a public entity);
4. Mixed ownership of implementation/execution and operation;
5. Private ownership, execution, and operation.

After the first review of these five scenarios by stakeholder S-2, it seems that the third scenario is the most favorable. This result was obtained with the help of the STAMP model and, with its control structure, delineated the first STPA step (see results in Table 6) and iterated safety/security communication and interaction protocols between stakeholders and actors using the STECA technique. This process made it easier for people who participated in the analysis to sharpen their focus and capture the essential parts of the system at this point; see a list of interviewees in Table A1 in Appendix A. Examples of questions and answers from interviewees are presented in Table A2 in Appendix B. During meetings with stakeholders and actors where the system-level constraints were scrutinized, the five scenarios were defined and analyzed. The scenario analysis included a closer look at the possibilities for minimizing the system risk and obtaining the most favorable ownership arrangement. This examination resulted in choosing scenario 3 as the best solution.

Scenario 3 involves private ownership and suggests that the project is financed with equity capital and a construction loan. The scenario also implies that the operation will be public and that access to household waste is guaranteed. The risk factors in this scenario, at this stage, are related to (1) social risk and (2) risks related to investors and contracts with them; projects like this offer green investment potential, but investors are likely to want to minimize their risk with a turnkey contract project arrangement. (A turnkey project is constructed such that it can be sold to any buyer as a completed product. The *Cambridge Dictionary* provides a definition of a turnkey contract: “A contract in which a company is given full responsibility to plan and build something that the client must be able to use as soon as it is finished without needing to do any further work on it themselves” [59].)

Table A3 in Appendix C is an extension of Table 6 and gives an overview of the feedback and actions needed for all 26 stakeholders listed in Table 6. The first column shows the stakeholder’s number (S-1–S-26), the fourth column shows the feedback (in Arabic numerals) received from another stakeholder (in square brackets), the fifth column shows the action (in lowercase alphabet letters) the respective stakeholder must provide to another stakeholder (in square brackets), and the last column shows a description for each action (equivalent in lowercase alphabet letters). The table setup is equivalent to the setup shown in Table 2, based on STECA.

As Table A3 illustrates, the STAMP system model of the project, developed with the STECA technique, is comprehensive and detailed. It is based on a systems theory and a systematic method that has been used in various projects in recent years. The sub-processes identified in the third column, marked in blue, have been identified by stakeholders and actors as system elements that need further modeling when a decision is made to undertake the project.

6. Discussion

In this study, a relatively new methodology and techniques and tools are proposed for achieving the objectives of a safety and security-based design of a major national infrastructure. It was tested on the example of a WtE project. In this, many academic fields were involved, i.e., safety science, risk analysis, project management, stakeholder theory, systems theory, and social science. The focus was on risk analysis and risk management. Designing

and building a major national infrastructure that is very costly, takes many years, and concerns all citizens of a country is a challenge. The project not only needs to be financed, but it must also be supported by both the public and politicians. If executed, the project would also be an important step in making Iceland sustainable in waste management.

In the study, SbD has been chosen as an engineering concept for risk management. It is a way to consider safety and security as much as possible from the beginning. Through communication, the SbD concept enables engaging different stakeholders throughout the development process and making their viewpoints and expectations understandable and transparent to each other.

The analysis methods and techniques of STAMP, STPA, and STECA were used to identify and evaluate actors and stakeholders, and appendant hazards and threats. They are based on systems theory and enable the development of a system model of the project. These methods have proven to be successful in analyzing complex systems. With STAMP, a system model of a WtE incineration plant was created including all influential stakeholders according to laws and regulations. In the beginning, however, only local authorities were considered to be internal stakeholders according to law, but since all the country's citizens and companies are buyers of waste management services, there are many stakeholders in this project. Only the country's general governmental system is excluded here, e.g., police and courts, since their involvement is only as general actors.

The results of the analysis of stakeholders and their roles, responsibilities, and necessary feedback and actions, are summarized in Tables 4 and 5, and an overview is given in Table A3 in Appendix C. These tables contain quite detailed information that has been confirmed in the study, as described in this article. Then, Figure 6 shows the system model of the entire project and the relationships of all stakeholders involved in it. The STPA software tool (first version) greatly facilitated the modeling work, which involved many iterations.

All the data obtained in this analysis work are important for the progress of the project. Based on this data, with the involvement of stakeholders, the fact was brought out that the most important thing at an early stage is to find the right composition for the project's owner group based on the requirements that will later become most significant in the operation of the WtE incinerator. Stakeholders came up with five possible scenarios, of which one was considered the best. This scenario (scenario 3) involves private ownership and that the project is financed with equity capital and a construction loan. The scenario also implies that the operation will be public and that access to waste is guaranteed. The risks are both social risks and risks related to investors and contracts with them. Projects like this offer green investment opportunities, but investors are likely to want to minimize their risk with a turnkey contract project arrangement. They are also likely to want the transparency and security that ISO audits and certification provide.

This study shows that the STAMP, STECA, and STPA hazard/threat analysis techniques can be applied in order to achieve safety and security-based design. These techniques can be used to identify stakeholders in a complex system and involve them and other actors in reviewing the system and its individual components. The system model serves as a basis for communication between stakeholders and actors and helps make not only their roles and responsibilities understandable and transparent, but also their viewpoints and expectations. STAMP, STPA, and STECA prove to be useful when analyzing a complex system/project and determining how best to design safety and security into a system.

In this study, the subject is a WtE incineration plant, which is an important sustainability project in any country. Figure 6 shows the system model of the project developed in this study. With the STAMP method, it was possible to identify 26 actors and stakeholders, some of which represent types of homogeneous stakeholders. They each have a role and responsibilities defined by laws and regulations. Only the municipalities can be considered internal stakeholders in the beginning since they carry responsibility for waste management

by law. It is up to the politically elected local authorities to decide if and when the project will be carried out.

Figure 6 also shows the necessary feedback each stakeholder needs for their actions in the system and shows the importance of the project owner (stakeholder S-3) as the main controller in the system. The controlled system, the actual WtE project, depends on that stakeholder. The responsibility for waste management that the municipalities carry (stakeholder S-1) is forwarded to the project owner. The municipalities are not able to execute the project on their own due to a lack of funds. The already existing SORPA Waste Municipal Association (stakeholder S-2) is not able to carry out the project, as the operating form of a municipal association does not allow the participation of private parties in the project and is subject to strict rules regarding tax and tender issues. It is not enough that there is political will to execute the project; private parties with enough resources are also needed to execute it, and the people of the country must look at the project positively and see their interest in it being addressed. Until now, there has been little progress in the project, but with the knowledge created in the preliminary project, carried out in 2021 [9], and in this case study, this might change. At this early stage, it is important to ensure that the project gets off to a good start, that risks are identified from the beginning, and that a suitable combination of owners is found, all while securing the funds and minimizing the project's risks. It is a prerequisite that other aspects of the project go well.

The decision-making process of the project, i.e., how to start the project and finance it and how to establish the owner group and share risk, is, however, complicated. There are many stakeholders and actors that influence the project in various ways, and they carry a variety of risk factors that need to be communicated and understood. These are both private and public parties, and their partnerships need to be carefully analyzed to find the optimal structure. The partnerships and all their prerequisites and criteria must be carefully thought out before the project begins. It must also be ensured that the legislation is sufficiently clear regarding tender requirements, possible competitive factors, material flows for incineration, and the division of responsibilities between municipalities and all the other parties involved in the project. There are two types of public bodies involved in the project, the local authorities and the governmental authorities, with politically elected representatives who are replaced at different times. The project also includes private parties and investors who will participate in the project after a decision has been made to go ahead with it. Only then can the actual preparatory work for the project begin, e.g., design and tendering. In the case discussed here, it is likely that known solutions in combustion technology will be able to be used. Less known is the technology of carbon capture and storage during operation.

This study shows that there is a need for a continuous and revised analysis of risk factors during the project's life cycle. After the WtE incinerator has been built and daily operations start, regular risk analysis and risk assessment must be carried out continuously, but this will most likely follow a standard process and be part of the internal control and coordinated management system of quality, safety, health, and environmental factors. To ensure reliability and credibility, it may be wise to build the management system based on international ISO standards and obtain accredited ISO certifications for the entire operation.

It is not a coincidence that all ISO management standards now require risk analysis as a part of decision making and good governance. The standards, however, do not give much guidance on how to conduct risk analysis. This study shows that the STAMP, STPA, and STECA techniques are effective when preparing big and complex projects that may take years to complete, like a WtE project. Their use helps to organize the project in an optimal way, also considering time factors. It supports decision making regarding both when and how it is best to take every step in the project. By identifying risk factors in time, it is possible to find ways to mitigate risk and make it manageable. This study confirms results from Bjerga et al. [53], who indicate that it provides a suitable approach to analyze risk in complex systems, with a focus on the treatment of uncertainty and potential surprises linked to the operation of complex systems. The application of ISO standards is a demand

of many investors who want to invest in green and environmentally friendly projects of this kind. Accredited certification of the project may, therefore, facilitate the financing of the project [18–20].

This study also reveals the great responsibility government and municipalities have regarding infrastructure projects like this one, to ensure there is an administration that finds the right channel for its preparation and all associated decisions. The law in Iceland is not clear in this regard, and this must, therefore, be considered a risk. One way to mitigate this risk would be to set up a special law for the project. There are precedents for this in the case of major national infrastructures, e.g., energy infrastructure.

7. Conclusions and Future Work

This study shows that STECA, as an early concept analysis variant of STPA, can be used to identify necessary stakeholders, analyze their responsibilities and roles, identify necessary feedback and control actions, and model the control structure of the system. This is, furthermore, an effective technique to integrate systemic safety and security into a major and complex infrastructure project like the WtE project studied in this article. The results show that the current mandatory administrative structure of a municipality association is not suitable as a governance structure for this kind of project. Municipalities have a legal obligation to dispose of waste in a sustainable way, but they have limited funds for large and costly projects like this one. This means that municipalities must participate in the project and be responsible for it according to law, but they cannot execute the project alone. They are public entities and are exempt from tendering requirements. Other investors, however, must submit to tender requirements. The project is, however, a feasible investment option for long-term investors, like those managing pension funds or investment funds, who prefer a steady return on investment. As a “green” project, it is also a feasible investment opportunity for those who choose to invest in sustainable and environmentally friendly projects. It is, therefore, necessary to assess the potential scenarios of the WtE project and analyze its risk further regarding each possible participant and quantify the outcomes that could be expected from each. For example, the possible operating arrangements of owners and operators must be differentiated and analyzed. The results of this study show that it can be beneficial to establish the project owner of the WtE incineration plant as a limited liability and listed company, but the operator could be a public organization, owned by municipalities, that rents the incineration properties and runs the plant, and so be exempt from tender obligations. With scenario analysis, it is possible to analyze more precisely the implementation opportunities of this project. It is worth mentioning that legislation on a national incineration plant could guarantee such a project. There is an example of such legislation for Reykjavík Energy from 2013. The law on the establishment of the national grid (Landsnet) in the year 2004 as a concessionaire for electricity transmission and the operation of the main electricity system in Iceland with independent board members with sufficient knowledge and experience is an example of how to ensure the professional operation of an important high-tech infrastructure company.

The study, furthermore, shows the importance of continuous and revised analysis of hazards, threats, and risks during the project period. After the WtE incinerator is built and daily operations begin, regular risk analysis and risk assessment must be carried out continuously, but this will most likely follow a standard process and be part of the internal control and coordinated management system of quality, health and safety, and environmental factors. To ensure reliability and credibility, it may be wise to base the management system on international ISO standards and obtain accredited ISO certifications for the entire operation. This study shows that in combination, STAMP, STPA, and STECA are powerful analysis techniques that can be used in the early stages of project design and throughout the project for all critical decision making.

The limitation of this study lies in the data available at this early stage of the project. There is great uncertainty about most aspects of the project since no decision has been made regarding the location of the WtE incineration plant. Most people involved have a limited

view and understanding of the whole project and mainly look at the aspects that affect them. The representatives of the municipalities who sit in the town councils are the ones who have the most control over the project at the beginning. They are politically elected for four years, and in politics, there is a tendency to disagree on issues rather than to agree on decisions. Therefore, the opinions of the public, who are also voters, are important. It is also a limitation of this study that many people who have participated in this study have limited experience and understanding of the implementation of risk analysis and how best to use it for decision making.

The findings, however, show that there is a strong reason to further investigate the feasibility of this project. A former feasibility study shows that gate fees and the investment that the project requires are acceptable in comparison to the current costs. It is important to ensure transparency in a project like this, where many parties have interests.

This study contributes to safety science, risk management, and project management. It utilizes, in an important way, different fields of study to improve important infrastructure projects that concern scientists, and many others, a great deal.

In future work, the authors plan to further explore the benefits of using STAMP and STPA in the project management of this WtE project when the decision has been made to start it.

Author Contributions: Conceptualization, S.H.B.; methodology, S.H.B.; software, S.H.B.; validation, S.H.B., P.J., S.E.T., I.M.D. and H.T.I.; formal analysis, S.H.B.; investigation, S.H.B. and H.T.I.; resources, S.H.B.; data curation, S.H.B.; writing—original draft preparation, S.H.B.; writing—review and editing, S.H.B., P.J., S.E.T., I.M.D. and H.T.I.; visualization, S.H.B.; supervision, P.J.; project administration, S.H.B.; funding acquisition, S.H.B. All authors have read and agreed to the published version of the manuscript.

Funding: A part of this work, the development of an STPA software tool, was conducted as a research project within Eurostars (Project ID: E10663—EERMF; [58]), supported by the Icelandic Technology Development Fund (Project No.: 169003-0611; [60]) and the Swiss Commission for Technology and Innovation (Project No.: 15822.1 PFIW-IW; [61]). The STPA software concept was originally presented at the 5th European STAMP/STPA Workshop and Conference at Reykjavik University in Iceland, in September 2017 [57,62].

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved in accordance with the requirements of the Institutional Review Department of Reykjavik University (RU-DoE-Review-Board-Oct 2021, 28 October 2021).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data are contained within the article.

Acknowledgments: Thanks to the reviewers of this paper for their valuable comments.

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

Appendix A

Table A1 presents an overview of meetings and interviewees in this study. A total of 53 people, including stakeholders and actors, were directly interviewed or participated in meetings where the WtE project was presented and discussed. The first column shows an identification number for each interviewee, the second column shows the type of organization at which the interviewee works, the third column shows the occupation or the role of the interviewee within the organization, the fourth column shows the number of meetings that were held wherein the WtE project was discussed, and the fifth column shows how many working hours were spent (approximately) in the meetings. A total of 81 meetings were held and 455 working hours were spent.

Table A1. An overview of interviewees and meetings held while modeling the WtE project.

Id.	Organization	Occupation/Role	No. of Meetings	No. of Hours
P-01	University	Professor	1	1
P-02	Engineering company	CEO	1	1
P-03	University	Professor	8	29
P-04	University	Professor	4	4
P-05	University	Professor	1	4
P-06	Ministry of the Environment	Head of department	1	1
P-07	Director of planning committee	Director	1	1
P-08	Environmental consulting company	Director	3	10
P-09	Engineering organization	Director	1	5
P-10	Accounting firm	Head of department	1	1
P-11	University and engineering agency	Professor	1	1
P-12	Waste processing organization	CEO		36
P-13	Waste processing organization	CFO		36
P-14	Waste processing organization	Head of department		22
P-15	Waste processing organization and politician	Board member		22
P-16	Waste processing organization and politician	Board member	11	22
P-17	Waste processing organization and politician	Board member		22
P-18	Waste processing organization and politician	Board member		22
P-19	Waste processing organization and politician	Board member		22
P-20	Waste management organization	Manager		18
P-21	Waste management organization	Manager	9	14
P-22	Law firm	Attorney		5
P-23	Law firm	Attorney	4	5
P-24	Law firm	Attorney	1	1
P-25	Financial organization	Head of department		1
P-26	Financial organization	Specialist	1	1
P-27	Municipality	Mayor		3
P-28	Municipality	Mayor		3
P-29	Municipality	Mayor		3
P-30	Municipality	Mayor	3	3
P-31	Municipality	Mayor		3
P-32	Municipality	Mayor		3
P-33	University	Professor	2	16
P-34	European WtE incineration plant	CEO		7
P-35	European WtE incineration plant	Specialist	1	7
P-36	European WtE incineration plant	CEO	1	7

Table A1. *Cont.*

Id.	Organization	Occupation/Role	No. of Meetings	No. of Hours
P-37	European WtE incineration organization	Managing director	1	1
P-38	University	Professor		5
P-39	University	Professor	4	17
P-40	Environmental consulting company	CEO		7
P-41	Engineering company	Head of department	7	7
P-42	Engineering company	Expert		7
P-43	Municipality	Mayor		1
P-44	Municipality organization	Expert	2	1
P-45	Waste processing company	CEO		1
P-46	Consultancy company	Manager		6
P-47	Consultancy company	Manager		6
P-48	Consultancy company	Manager	6	6
P-49	Consultancy company	Analyst		6
P-50	Consultancy company	Analyst		6
P-51	Consultancy company	Consultant		6
P-52	University	Professor	4	9
P-53	Governmental institution	CEO	1	1
Total:			81	455

Appendix B

Table A2 shows examples of questions asked and answers received in interviews with stakeholders and actors while working on the STAMP model for the WtE incineration plant in this study.

Table A2. Examples of questions asked and answers received in this study.

No.	Questions	Answers
1	How does the status/responsibility of individual municipalities [S-1] change after the WtE Project Owner [S-3] has been established?	P-01: The municipalities [S-1], the local authorities, are ultimately responsible according to law, they are responsible in contracts regarding the construction.
2	Does the Ministry of the Environment, Energy and Climate [S4] need technical information regarding the proposed WtE project from the WtE Project Owner [S-3], the design manager [S-17], or the engineers [S-19]?	P-04: If the electrical power from the WtE plant is 10 MW or more, the plans need to be reviewed by the electrical power framework committee, according to law. The WtE plant must be connected to the electrical grid [S-24]. P-01: The project plan must not be reviewed by the Ministry of the Environment, Energy and Climate [S-4].
3	Who needs to review or approve an environmental assessment other than the municipality licensor [S-10] that grants the construction permit and the National Planning Agency [S-7]?	P-01: Basically, these two parties, but sometimes there are requirements in laws regarding whom the Planning Agency has to contact and ask for their opinions.
4	Which public bodies must be informed about the project?	P-07: The building official is part of the relevant municipality [S-10]. P-01: The construction process must be followed, the project concerns notifiable construction, the project has to go through a review process (according to the Aarhus Agreement, it is a citizen's right to be informed), one has to be prepared for appeals from the public [S-22].
5	What information or feedback does the Environment Agency of Iceland [S-5] need to grant a work/project permit?	P-01: The "building regulation" frames authorizations (see: https://www.byggingarreglugerd.is/ , accessed on 12 November 2023).

Table A2. Cont.

No.	Questions	Answers
6	Does the license provider (a municipality [S1, S-10]) himself have to carry out an investigation into accidents or mishaps that may occur?	P-02: The Administration of Occupational Safety and Health carries out the investigation in case of an accident. It is a part of the standard public regulatory framework (out of scope, not considered a stakeholder).
7	The role of the Regulatory body for buildings and constructions [S-9] is limited (monitoring)—is it right to include this organization in the STAMP system model?	P-11: Yes. P-04: Yes.
8	Is an “incident report” an output from an investigation process? Who manages or directs such an accident investigation process?	P-02: The requirements of “The Administration of Occupational Safety and Health” governs what incidents must be investigated and what reports given after accidents of any kind (out of scope, not considered a stakeholder).
9	In the construction regulation, it says about execution control: “The licensor carries out external control”. Is the “Regulatory body for buildings and constructions” [S-9] also involved in supervision?	P-02, P-07: The external control is in the hands of the municipality that grants the building permit [S-10]. The role of the regulatory body [S-9] is to monitor that laws and building regulations are followed, if there is a suspicion that this is not the case.
10	Should the Road and Coastal Administration [S-8] be a part of the STAMP system model?	P-03, P-04: Yes.
11	Has there been sufficient differentiation between internal and external auditors in the STAMP system model?	P-03: Yes. P-02:
12	Does the WtE Project Owner [S-3] (building licensee) take care of the final inspection and safety inspection on the construction site—or is this “auditing” role outsourced to others (in contracts with the Project Owner)?	<ul style="list-style-type: none"> - Owner’s engineer, also known as the client’s engineer, is a term often given to the representative of the commissioning company of a construction or engineering project. It is a subcontracted role; undertaken to protect the owner’s interests by ensuring that the technical and build contractors are adhering sufficiently to the project specification. - The Project Owner is responsible for carrying out the mandatory supervision of the construction of a structure in accordance with the provisions of the Act on Structures and this regulation, regardless of scope categories. - Building control is divided into internal control, which is the responsibility of the owner, and external control, which is carried out by inspectors. Supervision is then divided into supervision of the design of structures on the one hand and supervision of implementation on the other hand. - The design manager [S-17] takes care of the owner’s internal control of the design of the structure, while the construction manager, as the owner’s professional representative, takes care of the internal control of the implementation on his behalf from the time the building permit or permit is issued until the final assessment has been carried out. The licensor carries out external monitoring to ensure that the design of the structure is in accordance with the provisions of “the Act on Structures”. The licensor is permitted to outsource supervision during the review of special plans in the case of difficult or extensive construction. - The inspector carries out status inspections [according to 3.7.3. art.] and performs security and final audits [according to 3.8. and 3.9. chapter]. - In the case of a public project, the governmental property agency must have a performance evaluation carried out, which states how the project has been carried out according to the plan, together with a comparison with similar projects if possible. It must be available no later than 6 months after the completion of the work.

Table A2. Cont.

No.	Questions	Answers
13	Does the main contractor [S-15] take care of tendering and selection of subcontractors?	P-02: Yes. Often, the project's tender documents specify that the main contractor should name several possible subcontractors, especially in specialized aspects, such as the supply of special equipment. Ultimately, however, the selection of subcontractors [S-16] is the responsibility of the main contractor [S-15].
14	What is the most complex and risky part of this project?	P-02, P-03, P-04, P-07, P-08, P-09, P-10, P-12, P-15-P19, P-27-P32: The most difficult part in a project like this one is to get the country's municipalities [S-1] (including the owners of the WMA [S-2], which are among Iceland's largest municipalities) to commit to the project and approve it (sub process1). Although the project is technical, politicians make the decisions about it. This creates a lot of uncertainty. It is important that the Icelandic state [S-11] participates in the project, but also there is great uncertainty. There is uncertainty regarding the form of project ownership [S-3] (sub process2) and financing of the project [S-1, S-11, S-13, S-14]. There is also uncertainty regarding the permit process (sub process8) until a construction/building permit is obtained. It may take years (with municipal elections in between). Many institutions, both governmental and within the municipality that grants the building permit, need to assess the impact of the project, i.e., due to environmental impact, zoning plan issues, health issues and traffic issues.
15	What information/feedback can the EU [S-12] receive on necessary legislation regarding to WtE issues from stakeholders? How can information be given to EU institutions?	P-06: Iceland has observer representatives in various EU working groups [S-12] in the climate field. The European IPPC Bureau is a cooperation platform between the governments of the EEA countries and the European business community. The European Integrated Pollution Prevention and Control Bureau (EIPPCB) is part of the Circular Economy and Industrial Leadership Unit of Directorate B—Growth and Innovation, one of six scientific directorates of the European Commission's Joint Research Center (JRC). Best Available Techniques (BAT) reference documents (BREFs) represent the outcome of the 'Seville process'. BAT should ensure that certain developed and tested technologies are used in environmental matters, which should be the best available technology available, the best for use. Iceland's participation is through Nordic cooperation, i.e., through the Nordic Council of Ministers (https://eippcb.jrc.ec.europa.eu/reference , accessed on 12 November 2023). P-01 confirms information given by P-06.
16	The "The Administration of Occupational Safety and Health" is a public institution that would only be involved in matters in case of a health and safety incident or accident. Should this institution be included in the STAMP system model?	P-02, P-03: No. The requirements of "The Administration of Occupational Safety and Health" governs what incidents must be investigated and what reports given after accidents of any kind. This organization is not a direct participant in a project, not rather than other public organizations, e.g., Data Protection Authorities, Police, and the Directorate of Labour. Out of project scope, not considered a stakeholder in the STMP system model.

Appendix C

Table A3 shows an overview of the STECA analysis on which the STAMP model of the WtE system is based. The table is an extension of Table 6.

Table A3. Overview of the STECA analysis.

Stakeholder Id.	Name of Stakeholder	Responsibility	WtE Incineration Plant—PPP Project—Preparation and Construction Phase				
			Feedback Needed [from Stakeholder(s) (Id.)]	Control Action [to Stakeholder(s) (Id.)]			
S-1	Municipalities	<ul style="list-style-type: none"> Legal obligation to dispose of waste in a sustainable way Responsibility for establishing the proper governance in the preparation and early decision-making phase of the project Project feasibility study Project risk assessment Responsibility for financing the whole project Establishing the PPP partnership for the project Supervisor role 	<ul style="list-style-type: none"> Analysis of technical possibilities to dispose of waste in a sustainable way [S-2, S-19] Results of a feasibility study [S-2, S-19] Estimates future cost without project [S-2, S-19] Financial backup or guarantee [S-9, S-13, S-14] Financial progress reports during project time [S-3] Public opinion [S-22] 	<ul style="list-style-type: none"> (a) Approval of the project (sub-process) [S-3] (b) Establish WtE Ltd. as a project owner (sub-process) [S-3] (c) Responsibility for the project transferred to project owner [S-3] (d) Location decision for the WtE plant [S-3] 	<p>(a) The approval of the project is both an output of the approval sub-process that is partially prepared by S-2 (in a pre-phase of the project) and a requirement. This is an output of the approval sub-process and a special establishment sub-process, but also a requirement. The WtE Ltd. will be formed if and when all the main municipalities in the country are ready to unite on the project—and if Minister for the Environment and Natural Resources (Ireland supports the project—and if (potential) investors, S-11, have been found. This is an output of the approval sub-process and a requirement.</p> <p>(b) This is an output of the approval sub-process and a requirement.</p> <p>(c) The approval of the project is both an output of a sub-process managed by S-2. A one-time output of the feasibility study but must be reviewed and confirmed by S-3 once the project starts. A design requirement. A one time output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts. A design requirement.</p> <p>(d) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(e) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(f) An output of the feasibility study, but project's risk must be re-assessed by S-3 once the project starts—and during design and construction phase.</p> <p>(g) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(h) This is a requirement; S-3 will take over once project starts.</p> <p>(i) This is a requirement; S-3 will take over once project starts.</p>		
		S-2	WMA—Waste Municipal Association	<ul style="list-style-type: none"> Serves the municipalities in establishing the WtE project Knowledge source 	<ul style="list-style-type: none"> Intentions of municipalities [S-1] Public opinion [S-22] 	<ul style="list-style-type: none"> (a) WtE feasibility study (sub-process) [S-3] (b) Estimates amount of waste into WtE incineration plant [S-3] (c) Estimates composition of waste into WtE incineration plant [S-3] (d) Preliminary project plan [S-3] (e) Preliminary business plan [S-3] (f) Results from preliminary project risk assessment [S-3] (g) Overview of legal requirements for WtE incineration plant [S-3] (h) Informs authorities about the intended project [S-4, S-5, S-7] (i) Informs the public through web site and social media [S-22] 	<p>(a) The WtE feasibility study is an output of a sub-process managed by S-2. A one-time output of the feasibility study but must be reviewed and confirmed by S-3 once the project starts. A design requirement. A one time output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts. A design requirement.</p> <p>(b) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(c) An output of the feasibility study, but project's risk must be re-assessed by S-3 once the project starts—and during design and construction phase.</p> <p>(d) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(e) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(f) An output of the feasibility study, but project's risk must be re-assessed by S-3 once the project starts—and during design and construction phase.</p> <p>(g) An output of the feasibility study, but must be reviewed and confirmed by S-3 once the project starts.</p> <p>(h) This is a requirement; S-3 will take over once project starts.</p> <p>(i) This is a requirement; S-3 will take over once project starts.</p>

Table A3. Cont.

WIE Incineration Plant—PPP Project—Preparation and Construction Phase					
Stakeholder Id.	Name of Stakeholder	Responsibility	Feedback Needed (from Stakeholder(s) (Id.))	Control Action (to Stakeholder(s) (Id.))	Description of Control Action (CA)
S-3	WIE Ltd.—project owner	<ul style="list-style-type: none"> Project owner (PPP affiliate) Project management, including reg. quality, health and safety, environmental and sustainability requirements Ensures project financing Daily supervision during project time Appoints a design manager Appoints a construction manager Assigns auditors Applies for a construction permit for the intended project and provides the necessary data, e.g., environmental assessment 	<ul style="list-style-type: none"> Results from a preliminary project plan [S-2, S-19] Results from a preliminary business plan [S-2, S-19] Results from a preliminary risk assessment [S-2, S-19] Project progress reports [S-15] Reports from auditors [S-21] Public opinion [S-22] 	<ul style="list-style-type: none"> (a) Environmental impact assessment (sub-process4) [S-10] (b) Application for WIE plant, building permit application and building documents (sub-process5) [S-10] (c) Signs contracts with clear split of responsibility [S-1, S-10, S-17, S-18, S-19, S-20, S-21] (d) Starting the project [S-10, S-15, S-22] (e) Business plan [S-10, S-15, S-17, S-18] (f) Tendering the project (main contractor) [S-15, S-16] (g) Chooses main contractor and sign contract [S-15] (h) Informs the public through web site and social media [S-22] (i) Informs authorities about the project [S-4, S-5, S-7] (j) Seeks / monitors public opinion [S-22] (k) Assigns auditors [S-10, S-21] 	<ul style="list-style-type: none"> (a) This is a one-time output of an environmental assessment process conducted by project owner and a requirement. (b) This is a one-time output of the building permit application. (c) This is an output. (d) This is a one-time output. (e) This is an output from feasibility study (from S-2), reviewed by S-3 and maintained as a "live" project plan, constantly reviewed through the project time. Also a requirement. (f) This is an output from feasibility study (from S-2), reviewed by S-3 and maintained as a "live" project plan, constantly reviewed through the project time. Also a requirement. (g) This is both a one-time output and a requirement. (h) This is both a one-time output and a requirement. (i) This is a continuous CA. (j) This is a continuous CA. (k) This is a requirement.
		<ul style="list-style-type: none"> Waste matters in accordance with the provisions of the regulatory framework for waste management, i.e., obligations under EEA law 	<ul style="list-style-type: none"> Information reg. location of WIE plant [S-3] Information reg. environmental and health issues [S-3] Technical information reg. WIE plant [S-3, S-17] 	<ul style="list-style-type: none"> (a) Supports the project in public [S-3, S-10] (b) Supports a possible application for a state guarantee [S-3] 	<ul style="list-style-type: none"> (a) This is a continuous CA and a requirement. (b) This is a CA (may be possible).
		<ul style="list-style-type: none"> Enforces laws on pollution prevention, environmental responsibility, nature conservation, and hygiene—sets environmental regulation Issuance of operating license for the WIE plant 	<ul style="list-style-type: none"> Project progress reports [S-3] 	<ul style="list-style-type: none"> (a) Grants an operating license at the end of the project [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement and an output that needs to be renewed/maintained.
		<ul style="list-style-type: none"> Provides harbor facilities for shipping to and from WIE plant location Examines conditions for harbor construction 	<ul style="list-style-type: none"> Location of the WIE incineration plant [S-3] Design requirements [S-3, S-17] Materials and quantities for shipping [S-3, S-17] 	<ul style="list-style-type: none"> (a) Builds a harbor near the WIE plant (sub-process6) [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement and a one-time output (needs maintenance from time to time).

Table A3. Contd.

WIE Incineration Plant—PPP Project—Preparation and Construction Phase					
Stakeholder Id.	Name of Stakeholder	Responsibility	Feedback Needed [from Stakeholder(s) (Id.)]	Control Action [to Stakeholder(s) (Id.)]	Description of Control Action (CA)
S-7	National Planning Agency	<ul style="list-style-type: none"> • Implementation of laws and regulations on environmental assessment of projects and plans • Presents the project owner's assessment plans and environmental assessment reports • Issues an opinion on assessment plans and on the environmental assessment of a project based on the developer's environmental assessment report and comments received on it 	<ul style="list-style-type: none"> • Environmental impact assessment [S-3] 	<p>(a) A written statement (opinion) regarding the assessment plans and the environmental assessment of a project based on the developer's environmental assessment report and comments received on it [S-3, S-10]</p>	<p>(a) This is a requirement and a one-time output.</p>
S-8	The Road and Coastal Administration	<ul style="list-style-type: none"> • Determines the roadway • Negotiates with landowners • Road design 	<ul style="list-style-type: none"> • Location of WIE incineration plant [S-3] • Location of WIE harbor [S-3, S-6] 	<p>(a) Road construction (sub-process7) [S-3]</p>	<p>(a) This is a requirement and a one-time output (needs maintenance from time to time).</p>
S-9	Regulatory body for buildings and constructions	<ul style="list-style-type: none"> • Monitoring of the implementation and compliance with laws and regulations reg. buildings and constructions • Investigation of whether building regulations are violated or not followed • Operation of a database for information on buildings and construction 	<ul style="list-style-type: none"> • Notification if law or regulation is violated [S-10, S-18] 	<p>(a) Monitoring of the implementation of the law on buildings and constructions [S-3]</p>	<p>(a) Monitoring is a legal requirement.</p>
S-10	Building licensor (municipality /landowner) of WIE construction site (many sub-institutions, fire brigade, health committee, planning committee, and politicians)	<ul style="list-style-type: none"> • Review of building permit application and building documents • Confirming consistency in the regional development plans • Grants a building permit • Investigation of major accidents and injuries, if and when they occur • Work status checks 	<ul style="list-style-type: none"> • Main drawings and building description documents [S-3, S-19] • Consent of co-owners or other parties as appropriate [S-1, S-13] • Work progress plan [S-3] • Signed declaration of responsibility from master builder etc. responsible for individual work components [S-15, S-16] • Design manager's overview of internal control during the implementation of the design [S-17] • Design manager's overview of responsibilities of individual designers and their signature to confirm that this is a comprehensive overview [S-17] • Statement from the construction manager [S-18] 	<p>(a) Issuance of a building permit (sub-process8) [S-3]</p> <p>(b) Review of work status check reports [S-3]</p> <p>(c) The licensor carries out a safety and final audit in accordance with the provisions of the inspection manual and inspection list and issues certificates for them [S-3]</p> <p>(d) Launches an accident investigation [S-3]</p>	<p>(a) The building permit is a requirement and a one-time output of the building application and document review.</p> <p>(b) Work status checks are a requirement.</p> <p>(c) A safety and final audit report is a requirement and a one-time output at the end of the project.</p> <p>(d) An accident investigation is a legal requirement.</p>

Table A3. Contd.

WIE Incineration Plant—PPP Project—Preparation and Construction Phase					
Stakeholder Id.	Name of Stakeholder	Responsibility	Feedback Needed [from Stakeholder(s) (Id.)]	Control Action [to Stakeholder(s) (Id.)]	Description of Control Action (CA)
S-11	Parliament	<ul style="list-style-type: none"> Makes legislation reg. waste disposal, environment, health, and safety 	<ul style="list-style-type: none"> Legal requirements needed [S-4, S-12] 	(a) Legislation [S-1, S-3, S-10]	(a) The project needs to comply with legislation at all times. Changes in relevant legislation must be monitored. This is a requirement and a continuous CA.
S-12	European Union (EU)	<ul style="list-style-type: none"> Coordinates waste and environmental issues within the EU Working groups with the participation of individual countries 	<ul style="list-style-type: none"> Intendment and requirement of EU and EEA member states [S-4, S-5] 	(a) EU directives on waste and environmental issues [S-4, S-11]	(a) The project needs to comply with EU directives at all times. Changes in directives must be monitored. This is requirement and a continuous CA.
S-13	Investors	<ul style="list-style-type: none"> Co-finance 	<ul style="list-style-type: none"> Business plan [S-3] Financial progress [S-3] 	(a) Provides contractual capital [S-3]	(a) This is a requirement.
S-14	Banks	<ul style="list-style-type: none"> Co-finance 	<ul style="list-style-type: none"> Business plan [S-3] Investment need [S-3] Financial progress [S-3] 	(a) Provides loans with acceptable collateral [S-3] (b) Line of credit [S-3]	(a) This is a requirement, based on the output of the business plan and capital from investors. (b) This is requirement and a continuous CA during project time.
S-15	Main contractor	<ul style="list-style-type: none"> Human resources available when needed Necessary equipment available when needed Project management on site Tenders and selection of subcontractors Project risk assessment Coordination of subcontractors Assesses, monitors and manages risk on project site Finishes the project on time 	<ul style="list-style-type: none"> Project progress reports from subcontractors [S-16] Incident reports from subcontractors [S-16] Information reg. availability of necessary resources from subcontractors [S-16] 	(a) Subcontractors' tenders and agreements [S-16] (b) Regular project progress reports [S-3, S-18] (c) Delivers project (and individual) work packages safely and on time [S-3, S-10] (d) Registration of incidents and nonconformities [S-3, S-9, S-10, S-18] (e) Root cause analysis of incidents and nonconformities that happen on project site (sub-process) [S-3, S-9, S-10, S-18] (f) Incident reports [S-3, S18]	(a) This is a requirement and subcontractor agreements are outputs of the tender sub-processes. (b) This is a requirement and a regular output of management team. (c) This is a requirement and a regular output of management team. (d) This is a requirement and a regular output of management team. (e) This is a requirement and an output of incident review process. (f) This is a requirement and a regular output of management team.
S-16	Subcontractors	<ul style="list-style-type: none"> Subcontractors available on time Risk assessment for work packages carried out Professional knowledge and experience 	<ul style="list-style-type: none"> Project requirements in written main contracts [S-13] Timed work schedule [S-13] 	(a) Project progress reports [S-15] (b) Incident reports [S-15] (c) Delivers work packages safely and on time [S-15] (d) Involvement in project risk assessment [S-15]	(a) This is a requirement and a regular output of S-16 to S-15 to S-3. (b) This is a requirement and a regular output of S-16 to S-15 to S-3. (c) This is a requirement and a regular output of S-16 to S-15 to S-3. (d) This is a requirement and an output of a limited risk assessment.

Table A3. Contd.

WIE Incineration Plant—PPP Project—Preparation and Construction Phase					
Stakeholder Id.	Name of Stakeholder	Responsibility	Feedback Needed (from Stakeholder(s) (Id.))	Control Action (to Stakeholder(s) (Id.))	Description of Control Action (CA)
S-17	Design manager	<ul style="list-style-type: none"> Submission of design data/drawings for approval for a building permit application Compiles a report on the designer's area of responsibility and confirms with their signature that it is a comprehensive overview Handles the owner's internal control for the design of the construction Organization of coordination of design data 	<ul style="list-style-type: none"> Design data from individual engineers and designers [S-19] 	<p>(a) Compiles design data from individual engineers and designers [S-3, S-10]</p> <p>(b) Signing a compiled statement on the responsibilities of designers and confirmation (with sign) that the overview is comprehensive [S-3, S-10]</p> <p>(c) Internal control during the design phase [S-3, S-10]</p>	<p>(a) This is a requirement and an output of the design data compiling process.</p> <p>(b) The signature of a certified design manager is a requirement and a one-time output of the design process.</p> <p>(c) This is a requirement and a continuous CA.</p>
		<ul style="list-style-type: none"> Makes written agreement with the master craftspeople which they hire on behalf of the owner Carries out the owner's internal control from the time the building permit is issued until the final assessment has taken place Carries out phased audits according to the inspection manuals Professional representative of the Project Owner [S-3] Requests a final audit before the WIE plant is started Operation of a quality management system 	<ul style="list-style-type: none"> Operating license from the regulatory body for buildings and constructions [S-9] Written contract with project owner [S-3] 	<p>(a) Signed statement by the construction manager regarding responsibility for the project so that a building permit can be granted [S-3, S-10]</p> <p>(b) Internal control (phase evaluation) during the construction phase [S-3, S-10, S-21]</p> <p>(c) Request and be present at a safety assessment for parts that are finished and ready for use [S-3, S-10, S-21]</p> <p>(d) Requests a final audit on behalf of the project owner and ensures that all necessary documents are available during the audit [S-21]</p>	<p>(a) The signature of a certified construction manager is a requirement and a one-time output before the construction process starts.</p> <p>(b) This is a requirement and a continuous CA.</p> <p>(c) This is a requirement.</p> <p>(d) This is a legal requirement.</p>
		<ul style="list-style-type: none"> Business plan Risk analysis and risk assessment Information gathering Design of the WIE plant 	<ul style="list-style-type: none"> Project information and requirements [S-2, S-3] 	<p>(a) Technical and design plans for WIE plant [S-3]</p> <p>(b) Financial plan for WIE plant [S-3]</p>	<p>(a) This is a requirement and an output from the project plan</p> <p>(b) This is a requirement and an output from the business plan.</p>
S-20	Insurance companies	<ul style="list-style-type: none"> Insurance 	<ul style="list-style-type: none"> Need for insurance [S-3] Notification about loss, damage, and mishaps [S-3] 	<p>(a) Insurance benefits due to damages, financial losses and mishaps based on insurance contracts (sub-process10) [S-3]</p>	<p>(a) This is a requirement and an output from sub-process10.</p>
S-21	Auditors, inspection agencies, e.g., the Government Property Agency	<ul style="list-style-type: none"> Auditing standards and process Financial auditing Health and safety, quality, security, and environmental management auditing ESG auditing 	<ul style="list-style-type: none"> Project progress reports [S-3] Cost statement from project owner [S-3] Incident reports [S-3] 	<p>(a) Financial audit reports [S-3, S-10]</p> <p>(b) EGS audit reports [S-3, S-10]</p> <p>(c) Reports on health and safety, quality, security, and environmental management [S-3, S-10]</p>	<p>(a) This is a requirement and an output of an audit process.</p> <p>(b) This is a requirement and an output of an audit process.</p> <p>(c) This is a requirement and an output of an audit process.</p>

Table A3. Contd.

WIE Incineration Plant—PPP Project—Preparation and Construction Phase					
Stakeholder Id.	Name of Stakeholder	Responsibility	Feedback Needed [from Stakeholder(s) (Id.)]	Control Action [to Stakeholder(s) (Id.)]	Description of Control Action (CA)
S-22	The public	<ul style="list-style-type: none"> Approve of the project. Remain critically engaged 	<ul style="list-style-type: none"> Information reg. the project and project progress throughout the project time, esp. health and safety, and environmental issues [S-3] 	<ul style="list-style-type: none"> Project support [S-3] Ask critical questions [S-3] Provide restraint if there is a reason [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement and a continuous CA. (b) This is a requirement and a continuous CA. (c) This is a requirement and a continuous CA.
S-23	Parties of the labor market	<ul style="list-style-type: none"> Preserve peace in the labor market 	<ul style="list-style-type: none"> Information on wage-related issues [S-3, S-22] 	<ul style="list-style-type: none"> (a) Wage settlements [S-3] (b) Peace in the labor market [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement, but the project has only little influence on this. (b) This is a requirement, but the project has only little influence on this.
S-24	Electrical grid company	<ul style="list-style-type: none"> Provides a connection to an electricity transmission system through a substation Transmits electrical power generated by the WIE plant to buyers 	<ul style="list-style-type: none"> Project time schedule [S-3] Information on est. electrical power production [S-3] 	<ul style="list-style-type: none"> (a) Agreement on transmittance of electrical power through a grid system (sub-process1) [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement and an output of a negotiation from sub-process11.
S-25	Hot water distribution company	<ul style="list-style-type: none"> Provides a connection to the hot water distribution system Distributes the hot water coming from the WIE plant 	<ul style="list-style-type: none"> Project time schedule [S-3] Information on est. water temperature and quantity [S-3] 	<ul style="list-style-type: none"> (a) Agreement on distribution of hot water through a pipeline system (sub-process2) [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement and an output of a negotiation from sub-process12.
S-26	Concrete plants and farmac production units (buildings and roads)	<ul style="list-style-type: none"> Use of good and affordable additive building materials 	<ul style="list-style-type: none"> Est. amount of solid waste residues [S-3] Information reg. quality of solid waste residues [S-3] Est. price of solid waste residues [S-3] 	<ul style="list-style-type: none"> (a) Purchase agreements on solid waste residue as additives for the construction industry for buildings and roads (sub-process13) [S-3] 	<ul style="list-style-type: none"> (a) This is a requirement and an output of a negotiation from sub-process13.

References

1. Van Gelder, P.; Klaassen, P.; Taebi, B.; Walhout, B.; van Ommen, R.; van de Poel, I.; Robaey, Z.; Asveld, L.; Balkenende, R.; Hollmann, F.; et al. Safe-by-Design in Engineering: An Overview and Comparative Analysis of Engineering Disciplines. *Int. J. Environ. Res. Public Health* **2021**, *18*, 6329. [CrossRef] [PubMed]
2. Bouchaut, B.; Asveld, L. Safe-by-Design: Stakeholders' Perceptions and Expectations of How to Deal with Uncertain Risks of Emerging Biotechnologies in the Netherlands. *Risk Anal.* **2020**, *40*, 1632–1644. [CrossRef] [PubMed]
3. Hale, A.; Kirwan, B.; Kjellén, U. Safe by design: Where are we now? *Saf. Sci.* **2007**, *45*, 305–327. [CrossRef]
4. Van de Poel, I.; Robaey, Z. Safe-by-Design: From Safety to Responsibility. *Nanoethics* **2017**, *11*, 297–306. [CrossRef] [PubMed]
5. Miles, S. Stakeholder Theory Classification: A Theoretical and Empirical Evaluation of Definitions. *J. Bus. Ethics* **2017**, *142*, 437–459. [CrossRef]
6. Maignan, I.; Ferrell, O.C.; Ferrell, L. A stakeholder model for implementing social responsibility in marketing. *Eur. J. Mark.* **2005**, *39*, 956–977. [CrossRef]
7. Freeman, R.E.; Harrison, J.S.; Wicks, A.C.; Parmar, B.L.; de Colle, S. *Stakeholder Theory: The State of the Art*; Cambridge University Press: Cambridge, UK, 2010; ISBN 978-1-139-48411-4.
8. Fanelli, A.; Misangyi, V.F. Bringing Out Charisma: CEO Charisma and External Stakeholders. *AMR* **2006**, *31*, 1049–1061. [CrossRef]
9. Ingason, H.T.; Björnsdóttir, S.H.; Gislason, S.; Bjarnadóttir, H.J.; Rasmussen, N.T.; Jensson, P.; Karlsson, A.; Tryggvason, H.F.; Rafnsson, R.O. *Skýrsla um Forverkefni um Framtíðarlausn til Meðhöndlunar Brennanlegs úrgangs í stað urðunar/Report on a Preliminary Project on a Future Solution for the Management of Combustible Waste Instead of Landfill*; SORPA bs.: Reykjavík, Iceland, 2021. Available online: https://fundur.reykjavik.is/sites/default/files/agenda-items/forverkefni_um_framtidarlausn_til_medhondlunar_brennanlegs_urgangs_i_stad_urdunar.pdf (accessed on 25 December 2023).
10. Leveson, N. A new accident model for engineering safer systems. *Saf. Sci.* **2004**, *42*, 237–270. [CrossRef]
11. Leveson, N.G. Engineering a Safer World. 2011. Available online: <https://mitpress.mit.edu/books/engineering-safer-world> (accessed on 3 July 2008).
12. Leveson, N.G.; Daouk, M.; Dulac, N.; Marais, K. *Applying STAMP in Accident Analysis*; Working Paper. Massachusetts Institute of Technology, Engineering Systems Division: Cambridge, MA, USA, 2003. Available online: <https://dspace.mit.edu/handle/1721.1/102905> (accessed on 5 May 2021).
13. *ISO 9001:2015*; Quality Management Systems—Requirements. International Organization for Standardization (ISO): Geneva, Switzerland, 2015.
14. *ISO 14001:2015*; Environmental Management Systems—Requirements with Guidance for Use. International Organization for Standardization (ISO): Geneva, Switzerland, 2015.
15. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization (ISO): Geneva, Switzerland, 2022.
16. *ISO 45001:2018*; Occupational Health and Safety Management Systems—Requirements with Guidance for Use. International Organization for Standardization (ISO): Geneva, Switzerland, 2018. Available online: <https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/37/63787.html> (accessed on 12 November 2023).
17. Björnsdóttir, S.H.; Jensson, P.; de Boer, R.J.; Thorsteinsson, S.E. The Importance of Risk Management: What is Missing in ISO Standards? *Risk Anal.* **2022**, *42*, 659–691. [CrossRef]
18. Kim, N.K.; Rahim, N.F.A.; Iranmanesh, M.; Foroughi, B. The role of the safety climate in the successful implementation of safety management systems. *Saf. Sci.* **2019**, *118*, 48–56. [CrossRef]
19. Wu, W.; An, S.; Wu, C.-H.; Tsai, S.-B.; Yang, K. An empirical study on green environmental system certification affects financing cost of high energy consumption enterprises-taking metallurgical enterprises as an example. *J. Clean. Prod.* **2020**, *244*, 118848. [CrossRef]
20. Appolloni, A.; Chiappetta Jabbour, C.J.; D'Adamo, I.; Gastaldi, M.; Settembre-Blundo, D. Green recovery in the mature manufacturing industry: The role of the green-circular premium and sustainability certification in innovative efforts. *Ecol. Econ.* **2022**, *193*, 107311. [CrossRef]
21. Björnsdóttir, S.H.; Jensson, P.; Thorsteinsson, S.E.; Dokas, I.M.; de Boer, R.J. Benchmarking ISO Risk Management Systems to Assess Efficacy and Help Identify Hidden Organizational Risk. *Sustainability* **2022**, *14*, 4937. [CrossRef]
22. Fleming, C.H.; Leveson, N.G. Early Concept Development and Safety Analysis of Future Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 3512–3523. [CrossRef]
23. Frola, F.R.; Miller, C.O. *System Safety in Aircraft Acquisition*; Logistics Management Institute: Washington, DC, USA, 1984; Available online: <https://apps.dtic.mil/sti/citations/ADA141492> (accessed on 16 November 2021).
24. Kölln, G.C.; Klicker, M.; Schmidt, S. Comparison of hazard analysis methods with regard to the series development of autonomous vehicles. In Proceedings of the 2019 IEEE Intelligent Transportation Systems Conference (ITSC), Auckland, New Zealand, 27–30 October 2019; pp. 2969–2975.
25. Fleming, C.H. Safety-Driven Early Concept Analysis and Development. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2015. Available online: <https://dspace.mit.edu/handle/1721.1/97352> (accessed on 16 November 2021).
26. Fleming, C.H. *Systems-Theoretic Early Concept Analysis (and Development)*; MIT: Cambridge, MA, USA, March 2015. Available online: <http://psas.scripts.mit.edu/home/wp-content/uploads/2015/03/2015-STECA-Tutorial.pdf> (accessed on 12 November 2023).

27. Flyvbjerg, B. *The Oxford Handbook of Megaproject Management*; Oxford University Press: Oxford, UK, 2017; ISBN 978-0-19-104617-9.
28. Brookes, N.J.; Locatelli, G. Power plants as megaprojects: Using empirics to shape policy, planning, and construction management. *Util. Policy* **2015**, *36*, 57–66. [[CrossRef](#)]
29. Cole-Hunter, T.; Johnston, F.H.; Marks, G.B.; Morawska, L.; Morgan, G.G.; Overs, M.; Porta-Cubas, A.; Cowie, C.T. The health impacts of waste-to-energy emissions: A systematic review of the literature. *Environ. Res. Lett.* **2020**, *15*, 123006. [[CrossRef](#)]
30. De Titto, E.; Savino, A. Environmental and health risks related to waste incineration. *Waste Manag. Res.* **2019**, *37*, 976–986. [[CrossRef](#)]
31. Guðmundsdóttir, G.F.; Eðvaldsson, K.; Vilhjálmsson, D.E.; Jónsson, J.Ö.G.; Bergþórsdóttir, I.A.; Pétursdóttir, S. *Greining á þörf Sorpbrennslu-stöðva á Íslandi*; ReSource International ehf.: Reykjavík, Iceland, 2020; p. 83. Available online: <https://www.stjornarradid.is/library/02-Rit-skyrslur-og-skrar/Greining%20%C3%A1%20%C3%BE%C3%B6rf%20sorbrennslust%C3%B6%C3%B0va%20%C3%A1%20%C3%8Dlandi.%20%C3%BAtg%C3%A1fa%20nr.2.1%20afhent.pdf> (accessed on 20 November 2021).
32. Luo, C.; Ju, Y.; Dong, P.; Gonzalez, E.D.R.S.; Wang, A. Risk assessment for PPP waste-to-energy incineration plant projects in china based on hybrid weight methods and weighted multigranulation fuzzy rough sets. *Sustain. Cities Soc.* **2021**, *74*, 103120. [[CrossRef](#)]
33. Utama, W.P.; Wibowo, A.; Jumas, D.Y.; Rita, E.; Peli, M. Yulcherlina Risk allocation of PPP waste to energy projects in Indonesia: A research framework. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *930*, 012023. [[CrossRef](#)]
34. Wu, Y.; Xu, C.; Li, L.; Wang, Y.; Chen, K.; Xu, R. A risk assessment framework of PPP waste-to-energy incineration projects in China under 2-dimension linguistic environment. *J. Clean. Prod.* **2018**, *183*, 602–617. [[CrossRef](#)]
35. Cui, C.; Sun, C.; Liu, Y.; Jiang, X.; Chen, Q. Determining critical risk factors affecting public-private partnership waste-to-energy incineration projects in China. *Energy Sci. Eng.* **2020**, *8*, 1181–1193. [[CrossRef](#)]
36. Wang, L.; Zhang, X. Critical Risk Factors in PPP Waste-to-Energy Incineration Projects. *Int. J. Archit. Eng. Constr.* **2017**, *6*, 55–69. [[CrossRef](#)]
37. Xu, Y.; Chan, A.P.C.; Xia, B.; Qian, Q.K.; Liu, Y.; Peng, Y. Critical risk factors affecting the implementation of PPP waste-to-energy projects in China. *Appl. Energy* **2015**, *158*, 403–411. [[CrossRef](#)]
38. Danish, M.S.S.; Senjyu, T.; Zaheb, H.; Sabory, N.R.; Ibrahim, A.M.; Matayoshi, H. A novel transdisciplinary paradigm for municipal solid waste to energy. *J. Clean. Prod.* **2019**, *233*, 880–892. [[CrossRef](#)]
39. Casti, T. Waste to Energy in Denmark: Danish Legal Pathway to a Clean Waste to Energy. Master's Thesis, Faculty of Law, University of Oslo, Oslo, Norway, 2020.
40. Strano, L.; Pecoraro, D.V.; Pecoraro, N.; Gigli, C.; Amara, G. Communication as a Prevention Tool: A Key Lever for General Acceptance of the Role of Incineration (Waste-to-Energy) and Transformation plants towards Circular Economy. Paper Presented at the 23th International Trade Fair of Material & Energy Recovery and Sustainable Development, ECOMONDO, Rimini, Italy, 5–8 November 2019; Procedia Environmental Science, Engineering and Management, p. 8. Available online: http://www.procedia-esem.eu/pdf/issues/2019/no2/31_Strano_19.pdf (accessed on 15 November 2021).
41. Ghaebi Panah, P.; Hooshmand, R.-A.; Gholipour, M.; Bornapour, M. Urban microgrid ancillary service provision using plugin electric vehicle and waste-to-energy CHP. *J. Energy Storage* **2020**, *29*, 101413. [[CrossRef](#)]
42. Agaton, C.B.; Guno, C.S.; Villanueva, R.O.; Villanueva, R.O. Economic analysis of waste-to-energy investment in the Philippines: A real options approach. *Appl. Energy* **2020**, *275*, 115265. [[CrossRef](#)]
43. Ferdan, T.; Šomplák, R.; Zvirálová, L.; Pavlas, M.; Frýba, L. A waste-to-energy project: A complex approach towards the assessment of investment risks. *Appl. Therm. Eng.* **2015**, *89*, 1127–1136. [[CrossRef](#)]
44. Nordestgaard, P.M.; Arndt, C.H. AMAGER BAKKE: A steel building with the design challenge of creating a world famous recreational roof. *ce/papers* **2019**, *3*, 151–156. [[CrossRef](#)]
45. Bisinella, V.; Nedenskov, J.; Riber, C.; Hulgaard, T.; Christensen, T.H. Environmental assessment of amending the Amager Bakke incineration plant in Copenhagen with carbon capture and storage. *Waste Manag. Res.* **2022**, *40*, 79–95. [[CrossRef](#)]
46. ISO 31000:2018; Risk Management—Principles and Guidelines. International Organization for Standardization (ISO): Geneva, Switzerland, 2018.
47. Leveson, N.G.; Thomas, J.P. *STPA Handbook*; Leveson and Thomas. Massachusetts Institute of Technology: Cambridge, MA, USA, 2018. Available online: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf (accessed on 12 November 2023).
48. Fleming, C.H.; Leveson, N.G. Improving Hazard Analysis and Certification of Integrated Modular Avionics. *J. Aerosp. Inf. Syst.* **2014**, *11*, 397–411. [[CrossRef](#)]
49. Chaal, M.; Valdez Banda, O.A.; Glomsrud, J.A.; Basnet, S.; Hirdaris, S.; Kujala, P. A framework to model the STPA hierarchical control structure of an autonomous ship. *Saf. Sci.* **2020**, *132*, 104939. [[CrossRef](#)]
50. Sultana, S.; Okoh, P.; Haugen, S.; Vinnem, J.E. Hazard analysis: Application of STPA to ship-to-ship transfer of LNG. *J. Loss Prev. Process Ind.* **2019**, *60*, 241–252. [[CrossRef](#)]
51. Friedberg, I.; McLaughlin, K.; Smith, P.; Laverty, D.; Sezer, S. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *J. Inf. Secur. Appl.* **2017**, *34*, 183–196. [[CrossRef](#)]
52. Dakwat, A.L.; Villani, E. System safety assessment based on STPA and model checking. *Saf. Sci.* **2018**, *109*, 130–143. [[CrossRef](#)]
53. Bjerga, T.; Aven, T.; Zio, E. Uncertainty treatment in risk analysis of complex systems: The cases of STAMP and FRAM. *Reliab. Eng. Syst. Saf.* **2016**, *156*, 203–209. [[CrossRef](#)]

54. Jamot, D.G.C.; Park, J.Y. System theory based hazard analysis for construction site safety: A case study from Cameroon. *Saf. Sci.* **2019**, *118*, 783–794. [[CrossRef](#)]
55. Sulaman, S.M.; Beer, A.; Felderer, M.; Höst, M. Comparison of the FMEA and STPA safety analysis methods—A case study. *Softw. Qual. J.* **2019**, *27*, 349–387. [[CrossRef](#)]
56. Fleming, C.; Leveson, N.G. Including Safety during Early Development Phases of Future Air Traffic Management Concepts. In Proceedings of the 11th USA/Europe Air Traffic Management Research and Development Seminar, ATM 2015, Lisbon, Portugal, 23–26 June 2015.
57. Rejzek, M.; Björnsdóttir, S.H.; Krauss, S.S. Modelling Multiple Levels of Abstraction in Hierarchical Control Structures. *Int. J. Saf. Sci.* **2018**, *02*, 94–103. [[CrossRef](#)]
58. Eureka | Eurostars Is Coming Back. Available online: <https://www.eurekanetwork.org/eurostars/> (accessed on 2 July 2021).
59. Cambridge Dictionary. Available online: <https://dictionary.cambridge.org/dictionary/english/turnkey-contract> (accessed on 23 June 2023).
60. Technology Development Fund. Available online: <https://en.rannis.is/funding/research/technology-development-fund/> (accessed on 2 July 2021).
61. Agency, I.-S.I. Innosuisse Is the Swiss Innovation Agency. Available online: <https://www.innosuisse.ch/inno/en/home.html> (accessed on 2 July 2021).
62. 5th European STAMP/STPA Workshop and Conference. Reykjavik University. Available online: <https://en.ru.is/stamp/> (accessed on 2 July 2021).

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

Article D

Modelling multiple levels of abstraction in hierarchical control structures

Special Issue Article: The 5th European STAMP Workshop (ESW) 2017, Chief Editor:
Svana Helen Björnsdóttir, Reykjavik University

Modelling Multiple Levels of Abstraction in Hierarchical Control Structures

Martin Rejzek^{1*}, Svana Helen Björnsdóttir², Sven Stefan Krauss¹

¹ *Safety-Critical Systems Research Lab, Zurich University of Applied Sciences;
Technikumstrasse 9; 8401 Winterthur; Switzerland; www.zhaw.ch/iamp/sks*

² *Stiki - Information Security; Laugavegur 178;
105 Reykjavík; Iceland; www.stiki.eu*

* *Corresponding author: martin.rejzek@zhaw.ch*

Abstract

The hazard analysis method “Systems Theoretic Process Analysis” (STPA) makes use of a functional system representation in the form of a Hierarchical Control Structure and uses this model as the starting point for the analysis process. The development of the Hierarchical Control Structure typically involves multiple iterations and starts at a rather abstract view, which is refined during the modelling process. Usually, no differentiation is made between the Hierarchical Control Structure model and its representation as a diagram. In addition, the representation is typically restricted to a single diagram. This paper addresses the opportunities of explicitly differentiating between model and views and introduces a concept encouraging use of multiple diagrams representing one model. This paper also discusses the rulesets and consistency considerations necessary to ensure the analysis is complete and the Hierarchical Control Structure representations are consistent with the model and with each other.

Keywords: STAMP, STPA, model, modelling, abstraction, diagrams, views

1. Introduction

Systems Theoretic Process Analysis (STPA) is an analysis method understanding safety and security as emergent properties of a system [1].

The typical analysis process of STPA, depicted in **Figure 1**, can be summarized as following:

- The system to be analyzed, first, needs to be described as a Hierarchical Control Structure (HCS) through the identification of controlling units (controllers), the controlled process, and the flow of control actions and feedback among them. The HCS represents a model of the system under analysis. Development of the Hierarchical Control Structure can be seen as preparation work before performing the STPA.
- In the first step of the analysis, referred to as “STPA Step 1”, inadequate control actions are systematically identified and described, and an assessment made about whether they can potentially result in a hazard, making them “unsafe control actions”.

- In the second step of the analysis, “STPA Step 2”, the reasons are systematically analyzed for why inadequate control actions that result in unwanted process outcomes can occur, and the corresponding scenarios are identified.

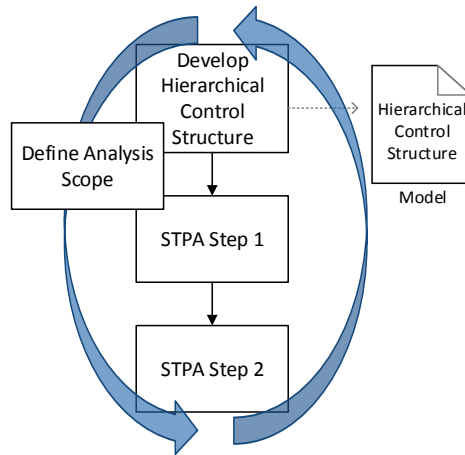


Figure 1: The STPA process is an iterative process (depicted by the blue arrows). The definition of the analysis scope takes place while developing the Hierarchical Control Structure (preparatory step of STPA), but also through STPA Step 1 and Step 2.

1.1. Problem Statement

Typically, the first HCS draft models the system to be analyzed, at a rather abstract level, in the form of a single diagram and refrains from establishing system details.

Such an abstract representation may feature, for example, “traffic control” as single controller, while not modelling the internals of the traffic control system individually. (Further examples of different levels of abstractions can be seen in [2, 3]). Some reasons for starting at an abstract level are as follows (non-exhaustive list):

a) As with every hazard analysis method and also for STPA, the analysis scope needs to be determined. Development of the HCS covers one aspect of this “scope definition”. Starting the modelling process at an abstract level allows for establishing a rough scope early in the process. While progressing through the analysis and refining the abstract representation, the scope will gradually become refined.

b) When a system is used in different applications, an analysis based on an abstract representation may serve as a common starting point for individual, application specific analyses, and refinements. Consider a robotic arm used to weld metal plates, but also used for exchanging tools of a milling machine. STPA can be performed for the robotic arm itself, not taking into account the specific application. This analysis can be used as starting point for further, application specific, analyses such as for the welding or tool exchange.

c) An abstract representation may even be valid for various types of systems. For example, the same abstract representation may be used to model cancer treatment with proton radiation beams [4-6] and brachytherapy [3]. This means existing models may be re-used and again serve as starting point for more concrete analyses.

d) Finally, starting the modelling process at an abstract level allows for quick identification of those parts of a system for which further clarification activities are

necessary. This is relevant, since such activities typically require time. The sooner the clarifications are initiated the better.

While progressing with the analysis the original abstract representation is typically “discarded”, i.e. it is no longer actively considered for STPA but instead more detailed, refined representations are used. Although the initial abstract representation might be kept as an informative resource (in the simplest form the analyst may keep a printout of the HCS diagram), STPA currently foresees no formal way of maintaining multiple levels of abstraction. This is considered a drawback of the methodology and frames the research objective of this paper.

1.2. Research Objective

This paper promotes making use of multiple diagrams to model the complete HCS. Furthermore, the paper shows what modelling rulesets and constraints need to apply in order to keep the diagrams, and subsequent STPA Step 1 and 2, consistent. In particular, the dependencies between the modelling elements appearing on the HCS diagrams as well as the dependencies of these elements to STPA Step 1 and 2 must be well traced and under control. Otherwise, model and analysis tend to become incomplete and inconsistent.

2. Proposed Concept and Use Cases

The concept described in this paper:

- Explicitly differentiates between the HCS “model” and it’s “views”;
- Provides the necessary ruleset for modelling HCS with multiple diagrams;
- Shows the influence on the process steps STPA Step 1 and 2 when using multiple diagrams.

As it turns out, the proposed concept doesn’t only enable modelling and analyzing multiple levels of abstraction as introduced in chapter 1, but it is also beneficial in other cases:

- Complementing Views: An analyst may use multiple diagrams to model different phases or characteristics of a system, for example, the phases *design*, *operation*, and *decommissioning*, or the characteristics *dose control* and *position control* of a cancer radiation treatment system¹. Principally the analyst can choose between the following options:
 - The phases or characteristics can be analyzed individually. However, this would result in neglecting the interactions between the phases/characteristics and be against the paradigm of STPA, as the holistic viewpoint would not be followed.
 - All phases or characteristics can be modelled by means of one HCS diagram. Depending on the size and complexity, the result could be a large and confusing representation.
 - Following the concept proposed in this paper: Multiple diagrams can be used to model the phases/characteristics where certain elements (controllers, control actions, etc.) could appear on multiple diagrams. All diagrams are part of the same model. Although multiple

¹ The instrumentation and control system in cancer radiation treatment systems for dose control may be quite different from the system for position control. Therefore, a desire may exist to handle dose control and position control individually from an analysis viewpoint.

diagrams represent the model, the analysis would see the system as a whole and would not handle the diagrams on an individual basis.

- **Intelligent Actuators and Sensors:** Once the analyst performs STPA Step 2, it can become clear that an element, which has been considered to be a simple actuator or sensor (therefore omitted on the HCS diagram), fulfills all the attributes of a STPA controller. For example, when an actuator configurable (e.g. an actuator which is programmable) and/or has the power to make decisions about the controlled process on its own.
 - The analyst can now go back to the original HCS diagram and add the intelligent actuator (where it would appear as “controller”) including the relevant control actions and feedback. (The resulting model would still contain only a single HCS diagram.)
 - Alternatively, the analyst can model the actuator and its control flow on a second HCS diagram. (The resulting model would then contain two HCS diagrams.)
- **Functional Redundancies:** Some systems make use of functional redundancies. An example of this is two ground based control centers for satellite control. While the control centers could be identical and impose the same strengths and weaknesses, their interconnectivity could lead to additional hazards.
 - The analyst can model the details of the identical ground centers on one diagram and use a second HCS diagram to model the control flow between the ground centers and the satellite.

3. Concept Development Process

The key factors stimulating HCS modelling by means of multiple diagrams are simple to state:

- Allow representation of a HCS by means of multiple diagrams (views);
- Allow using the same element in multiple diagrams;
- Allow parent-child relationship among elements.

However, as mentioned above, keeping the diagrams consistent and ensuring the STPA Step 1 and 2 match the model and are complete is not a trivial objective. The three diagrams in Figure 2 give an illustrative example of this complexity.

Diagram 1 in Figure 2 shows a hierarchical control structure with three controllers (labelled *A*, *B*, and *C*) and a *Controlled Process*. For the sake of this example only two control actions are explicitly shown: *CA1* and *CA2*. *Diagram 2* shows controllers *A*, *B* and the *Controlled Process* again. This diagram does not show *Controller C* and consequently control action *CA1* which is received by *Controller C*. *Diagram 3* shows a third view of the same model focusing on the internals of *Controller B*. Note that *CA1* appears on the first but does not appear on the second and third diagram. Furthermore, the source of *CA2* is *Controller B* in the first and second diagram while it is *Controller B.1* in the third diagram.

This brings up a couple of modelling and analysis questions. How is the analyst made aware of the fact that *Controller B* issues *CA1* when working with *Diagram 2*? Could the analyst show *CA1* on *Diagram 2* even though *Controller C* is not represented? Is it inconsistent to have *CA2* appearing on *Diagram 2* and *3* with different sources? How does *CA2* need to be handled in STPA Step 1 and 2?

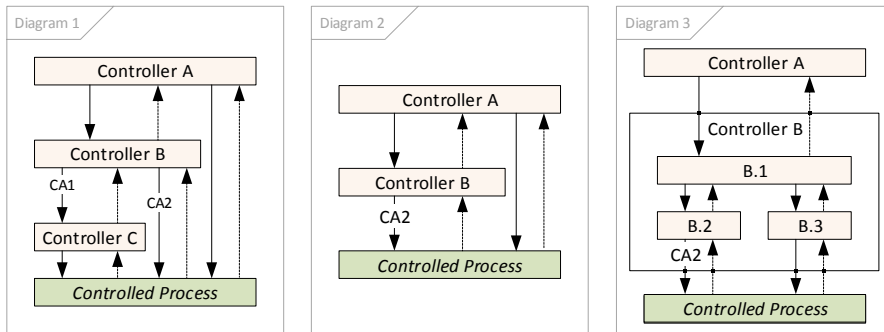


Figure 2: Representation of a Hierarchical Control Structure by means of three diagrams. In order to keep the diagrams consistent and making sure the analysis matches the model and is complete, a ruleset and consistency considerations are indispensable.

To ensure the diagrams are consistent and the analysis is complete, a set of rules and consistency considerations are indispensable - addressing not only the modelling aspect, but also STPA Step 1 and 2. The “divide and conquer strategy” illustrated in Figure 3 was used to derive rulesets and consistency considerations for the individual use cases and consolidate them into one set.

Identify Use Cases: As a first step, use cases have been identified, where using multiple HCS diagrams describing the same model will benefit the analysis. Some of these use cases have already been mentioned in chapter 2.

In a second step the use cases were mentally played through and analyzed with the help of knowledge gained from previous projects [4, 5, 7-10], literature and a constructed example. The aim of the constructed example was to analyze situations, which did not occur in previous projects nor the literature we looked at, but were principally possible.

For each use case the set of rules was derived that is necessary to enable the use case. The ruleset contains specifics about modelling and consistency considerations, as well as, rules influencing STPA Step 1 and 2.

Previous projects, literature, and additional examples were used to preliminary verify the applicability and correctness of the derived ruleset. (A proper verification is yet to be done.)

The individual rulesets were consolidated into one basic ruleset, with the rules and consistency considerations refined. This last step is still a work in progress.

The following two chapters discuss the two use cases “complementing views” and “levels of abstraction”.

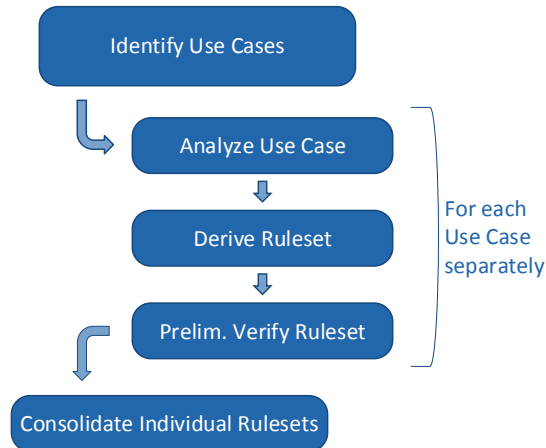


Figure 3: First, use cases were identified that benefited from using multiple Hierarchical Control Structure diagrams. Each use case was separately analyzed, a ruleset derived, and the ruleset preliminary verified. Finally, the individual rulesets were consolidated into one.

4. Complementing Views

4.1. Introduction to Complementing Views

Figure 4 provides an abstract example of complementing views. *Diagram 4a* and *4b* together represent the exact same model as *Diagram 4*, just in two separate diagrams.

Controller Q issues control action *CA1* that is received by *Controller R*. *Controller R* issues control action *CA2* that is received by *Process S*. Additionally, *Controller Q* influences the *Process S* directly by the means of control actions *CA3* and *CA4*. Feedback is not explicitly modelled in this example.

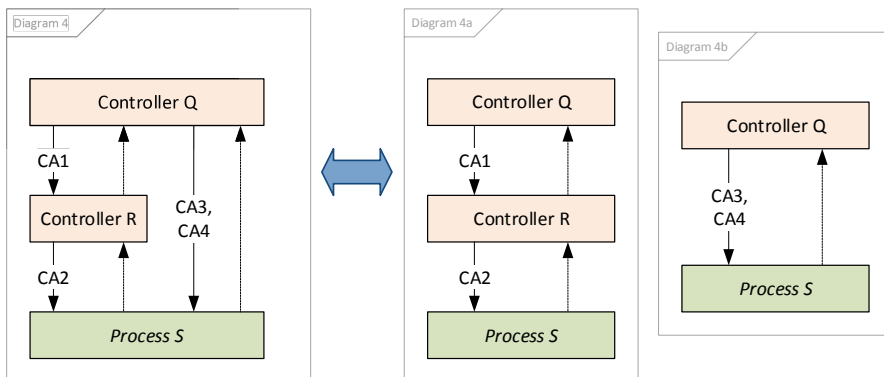


Figure 4: Diagram 4a and 4b together describe exactly the same model as Diagram 4 on the left side.

Table 1 lists the appearance of elements on *Diagram 4, 4a, and 4b* from Figure 4.

Element	Appearance in Figure 4		
	Diagram 4	Diagram 4a	Diagram 4b
Controllers:			
Controller Q	Yes	Yes	Yes
Controller R	Yes	Yes	No
Controlled Processes:			
Process S	Yes	Yes	Yes
Control Actions:			
CA1	Yes	Yes	No
CA2	Yes	Yes	No
CA3	Yes	No	Yes
CA4	Yes	No	Yes
Feedback:			

Table 1: Appearance of elements on Diagram 4, 4a, and 4b of Figure 4.

4.2. Ruleset for Complementing Views

The rules identified for this use case are simple and straight forward. A subset of those rules is provided in the following list:

- The same controller may appear on multiple diagrams.
- A diagram may show only a subset of the control actions generated/received by a controller.
- STPA Step 1 shall be performed for all control actions regardless of which diagram they are shown on.
- Every element (controller, controlled process, control action, or feedback) shall appear on one diagram at least.
- ...

While this rather basic use case can be beneficial to the analyst in certain circumstances, it is also a pre-requisite for all other use cases such as “levels of abstraction” addressed in the following chapter.

5. Levels of Abstraction

5.1. Introduction to Levels of Abstraction

The motivation to support different levels of abstraction when modelling the Hierarchical Control Structure has already been laid out in chapter 1. This use case is based on the premises that two visual representations of a controller exist:

- A representation that shows the controllers interaction with its environment. This view doesn’t show any internals of the controller, but it is represented as a black

frame from the hierarchical control structure viewpoint². We refer to this type as D0-representation. (Figure 5, controllers shown on the left diagram)

- A representation that shows the internals of the controller, referred to as D1-representation. In this representation, the decomposed controller is visualized as a frame, which allows refining it with new elements and their control flow. (Figure 5 “Treatment Delivery” on the right)

The example shown in Figure 5 is based on [4-6]. The example shows the D0- and D1-representations of the controller *Treatment Delivery*.

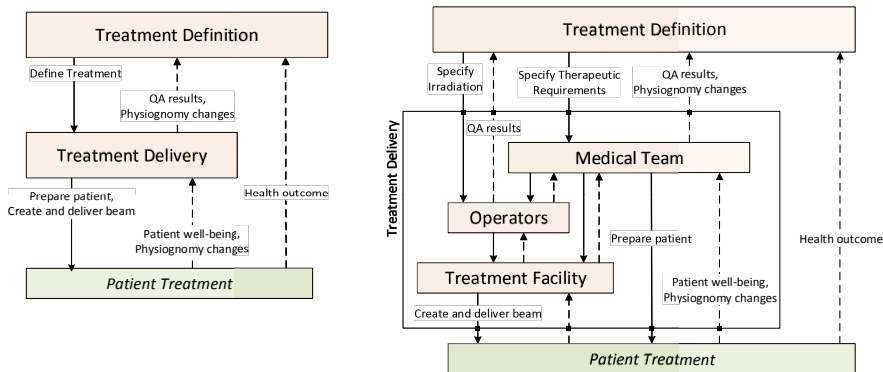


Figure 5: An example based on [4-6] showing two levels of abstraction of the controller “Treatment Delivery” and the control action “Define Treatment”. The structure shown on the right shows the internals of “Treatment Delivery”. Furthermore, on this side the control action “Define Treatment” is refined into “Specify Irradiation” and “Specify Therapeutic Requirements”.

While the left diagram of Figure 5 displays the controller *Treatment Delivery* as a single unit (D0-representation), the right diagram displays the internal details of the *Treatment Delivery* (D1-representation).” These internals are: *Medical Team*, *Operators*, and *Treatment Facility*. While the control actions *Prepare patient*, and *Create and deliver beam* are issued by the controller *Treatment Delivery* on the left, they are issued by *Treatment Facility*, respectively by the *Medical Team* on the right.

The concept of refinement does not only apply to controllers, but also to control actions and feedback. For example, the left diagram of Figure 5 shows the control action *Define Treatment*. This control action is not shown in the right diagram, but it is represented by *Specify Irradiation* and *Specify Therapeutic Requirements*. An overview about the refinement and relationship between controllers, control actions, and feedback is given below in Table 2.

² Internals like the process model, which the controller naturally contain are typically not shown graphically on the hierarchical control structure diagram.

Element		Appearance on Figure 5	
Parent element	Child element	Left diagram	Right diagram
Controllers:			
Treatment Definition		Yes	Yes
Treatment Delivery		Yes	As frame
	Medical Team	No	Yes
	Operators	No	Yes
	Treatment Facility	No	Yes
Controlled Processes:			
Patient Treatment		Yes	Yes
Control Actions:			
Define Treatment		Yes	No
	Specify Irradiation	No	Yes
	Specify Therapeutic Requirements	No	Yes
Prepare patient		Yes	Yes
Create and deliver beam		Yes	Yes
Feedback:			
QA results		Yes	Yes*
Physiognomy changes		Yes	Yes
Patient well-being		Yes	Yes
Physiognomy changes		Yes	Yes
Health outcome		Yes	Yes

* Feedback appears twice on the right diagram. Once linked to the Operators, once to the Medical Team.

Table 2: Appearance of elements in Figure 5.

5.2. Ruleset for Levels of Abstraction

Also for the use case “Levels of Abstraction”, a set of rules has been identified. For example, the following pair of rules:

- A feedback may have multiple sinks.
- If a feedback has multiple sinks, they must be related to each other by a parent-child relationship.

These two rules apply to the feedback *Patient well-being* of Figure 5. The sink of this feedback is the controller *Treatment Delivery* (left diagram) respectively, but more precisely, the controller *Medical Team* (right diagram) is related by a parent-child relationship with *Treatment Delivery*.

6. Conclusion and Outlook

While the rulesets for the individual use cases have been derived and a successful preliminary verification of them was conducted, the consolidation of the rules is still work in progress.

We believe the concept described in this paper is especially useful when an analysis shall dive into the details of a system. Making sure to comply with the ruleset and

constraints involves some effort; however, we believe this effort is highly automatable through software tools and does therefore not necessarily result in substantial additional workload for the analyst. Nevertheless, the analyst has to understand the basic concept of modelling HCS with multiple diagrams.

The ruleset and constraints allowing complementing views have successfully been implemented in a STPA software tool [11]. In a next step, the proposed concept will be applied from the start of an analysis project with STPA.

Acknowledgments

This work was conducted within research projects supported by the Swiss Commission for Technology and Innovation (project grant number 15822.1 PFIW-IW; [12]) and by Eurostars (project ID 10 663; [13]). The concept described in this paper formed a talk presented at the 5th European STAMP/STPA Workshop and Conference in Reykjavík, Iceland in September 2017. [14, 15]

References

- [1] Leveson, N.G., *Engineering a safer world: Systems thinking applied to safety*. 2012, Cambridge MA, USA: MIT Press.
- [2] Adesina, A.A., et al., *Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management*. *Pharmaceutical Medicine*, 2017. **31**(4): p. 267-278.
- [3] Pawlicki, T., et al., *Application of systems and control theory-based hazard analysis to radiation oncology*. *Medical physics*, 2016. **43**(3): p. 1514-1530.
- [4] Rejzek, M., *Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System*, in *STAMP Workshop 2012*. 2012: MIT, Boston.
- [5] Rejzek, M., *Evaluation of STPA in the Safety Analysis of the Gantry 2 Proton Radiation Therapy System ... a Review*, in *1st European STAMP Workshop*. 2012: Braunschweig.
- [6] Antoine, B., *Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry*. 2013, Massachusetts Institute of Technology.
- [7] Rejzek, M., *Use of STPA in digital instrumentation and control systems of nuclear power plants*, in *2nd European STAMP Workshop*. 2014: Stuttgart.
- [8] Rejzek, M., C. Hilbes, and S.S. Krauss, *Safety Driven Design with UML and STPA*, in *STAMP Workshop 2015*. 2015: MIT, Boston.
- [9] Krauss, S.S., M. Rejzek, and C. Hilbes, *Tool Qualification Considerations for Tools Supporting STPA*. *Procedia Engineering*, 2015. **128**: p. 15-24.
- [10] Krauss, S.S., M. Reif, and M. Moser, *CAST Analysis of a Railroad Accident in Switzerland*, in *5th European STAMP/STPA Workshop and Conference*. 2017: Reykjavik, Iceland.
- [11] *Risk Management studio (RM Studio)*. Available from: <http://www.riskmanagementstudio.com/>.
- [12] *Swiss Confederation - Commission for Technology and Innovation CTI*. Available from: <https://www.kti.admin.ch/kti/en/home.html>.
- [13] *European Commission - Eurostars*. Available from: <https://www.eurostars-eureka.eu/>.
- [14] *5th European STAMP/STPA Workshop and Conference*. Available from: <https://en.ru.is/stamp>.
- [15] *ESW: European STAMP Workshop*. Available from: <http://www.stamp-workshop.eu/>.

Article E

Can the “VUCA Meter” Augment the Traditional Project Risk Identification Process? A Case Study

Article

Can the “VUCA Meter” Augment the Traditional Project Risk Identification Process? A Case Study

Thordur Vikingur Fridgeirsson *, Helgi Thor Ingason *, Svana Helen Björnsdóttir and Agnes Yr Gunnarsdóttir

School of Engineering, Reykjavik University, Menntavegur 1, 101 Reykjavik, Iceland; svanahb@ru.is (S.H.B.); agnesyg1996@gmail.com (A.Y.G.)

* Correspondence: thordurv@ru.is (T.V.F.); helgithor@ru.is (H.T.I.)

Abstract: In this rapidly changing and fast-growing world, sustainability is an important paradigm. However, the constantly growing level of uncertainty leads to increased strain in decision making. This results in a growing need for a more effective and extensive approach for identifying project risk in particular events that are not easily detected but can have a severe impact, sometimes referred to as Black Swans or “fat tail” events. The VUCA meter is a normative approach to identify project risk by assessing in a structured way events that may be volatile, uncertain, complex, and ambiguous and might contribute to the project risk. In this study, the VUCA meter is benchmarked against a traditional risk identification process as recommended by PMI[®]. Firstly, two workshops, each referring to the respective risk identification method, were conducted. Secondly, a Delphi survey was run to investigate if the VUCA meter would capture Black Swan risk events that are bypassed by the traditional risk identification approach. The results clearly indicate that the VUCA meter can be developed to be a significant addition to the conventional risk identification process for large projects that are at an early stage. The VUCA meter facilitates a discussion that gets people to think beyond the traditional framework for identifying project risk factors. As a consequence, “fat tail” events, that are not apprehended with the conventional technique, are captured by the VUCA meter.

Keywords: project management; risk management; risk identification; risk assessment; VUCA



check for updates

Citation: Fridgeirsson, T.V.; Ingason, H.T.; Björnsdóttir, S.H.; Gunnarsdóttir, A.Y. Can the “VUCA Meter” Augment the Traditional Project Risk Identification Process? A Case Study. *Sustainability* **2021**, *13*, 12769. <https://doi.org/10.3390/su132212769>

Academic Editors: João Carlos de Oliveira Matias and Paolo Renna

Received: 21 October 2021

Accepted: 16 November 2021

Published: 18 November 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Vadlaheiðargöng project is a 7.5 km mountain tunnel at the north coast of Iceland connecting the city of Akureyri with Fnjoskadalur. The initial business model for the tunnel project was presented in 2002. It was assumed that the construction and the operation of the tunnel would be a private-public enterprise with high feasibility and limited technical difficulties [1]. Road tolls would recover all costs within 20 years plus a macroeconomic gain of 8% [2]. When market financing folded due to the international finance crisis in 2008, the arrangement was modified and the Icelandic government guaranteed a loan to make the construction possible. When the construction commenced, the Vadlaheiðargöng project soon hit some serious unforeseen problems. In the beginning of 2014, a major hot water leak, due to unexpected geothermal activity in the mountain, was detected making drilling impossible due to heat and steam. To be able to proceed, the contractor had to move the equipment to the other side of the mountain and continue drilling from there. Unfortunately, in April 2015, a major unexpected cold water leak was discovered on the new drilling site. The water completely floated the tunnel causing serious problems. A famous news clip from this period shows a TV reporter rowing a boat inside the tunnel to investigate the conditions. The tunnel was scheduled to be ready for traffic in 2016 (the initial plan assumed 2011). However, it was only operative in December 2018, more than two years later than planned [1]. The cost overrun in 2017 was estimated at 44%. However, it should be noted that in the presented cost overrun number, the cost of finance was not included and the real total cost overrun is thus much higher [3]. In July 2019, it was noted

that the income from the tolls was 35–40% less than expected [4]. Moreover, the COVID-19 pandemic resulted in a major breach in traffic volume in 2020, as the Icelandic tourist industry collapsed and local people were encouraged to limit their mobility as much as possible. This brief overview of a recent extensive infrastructure project is an appropriate prelude to a paper on a new method for assessing project risk in the modern fast changing and turbulent environment that is also urging for sustainable solutions.

We published our study on the VUCA meter, “The VUCA’ility of Projects; A New Approach to Assess a Project Risk in a Complex World” in the beginning of 2021 [5]. The study introduced a risk identification tool to supplement the conventional approach for risk assessment, advocated by international project management associations such as PMI (Project Management Institute). The initial idea assumes that we live in a VUCA business world [6] where volatility, uncertainty, complexity, and ambiguity prevail. In this rapidly changing environment, the need for a comprehensive risk identification process has become more remarkable and more significant in any project preparation [7]. The conventional risk assessment model is based on evaluating risk events based on two variables, the likelihood of the occurrence and the impact the risk event would have if it occurred. These two values are then used to rank the possible risk events to determine the most significant ones [8]. However, studies, such as Ackermann et al. [9], mention that the conventional approach used to identify and assess risk is too narrow and might not detect a “wider set of risks”. The short narrative on Vadlaheidargöng, earlier in this text, is descriptive for the “unknown unknowns” that a project planner can be confronted with. An international economic collapse, an unknown hot water vein, and an unknown cold water source effected the project lifecycle negatively. Furthermore, the COVID-19 pandemic almost wiped out the number of tourists visiting Iceland in 2020 reducing even further the expected tunnel traffic. It is questionable that the conventional approach would detect a low probability and high impact risk event such as the COVID-19 pandemic, political undercurrents caused by unconventional politicians such as president Trump, uncertainty in weather-related incidents due to climate changes, and so on. Furthermore, assessors and decision makers may have cognitive limitations to make judgments on probabilities, as was determined by the seminal work of Daniel Kahneman and Amos Tversky who published their findings in a series of papers in the early 1970s [10]. The central theme of their work is that people use simple mental strategies to cope with complex estimates and make judgments. This alone justifies further considerations of whether a traditional risk identification and assessment can be improved to ensure it covers possible risk factors in a more comprehensive way. Bent Flybjerg [11] has recommended the use of “reference class forecasting”, a forecasting method based on empirical evidence, to bypass the biases of human judgments [11]. The problem of the limitations of traditional risk management is, e.g., well documented by the influential work of Nassim Taleb [12,13]. Low probability and high impact events are often referred to as “Black Swan” events and the fallacy of overlooking them is named the “ludic fallacy”. The ludic fallacy states that decision makers might ignore small variations in the data that could have huge impact. This is also referred to as “fat tail risk”, referring to the tails of the normal distribution—located several standard deviations from the mean [13]. Taleb [12] defines a Black Swan as an event meeting three criteria: (a) it is an outlier as it lies outside the realm of regular expectations, (b) it carries extreme impact, and (c) human nature makes us put together explanations for its occurrence afterwards, making it seem explainable and predictable.

In response to the need to seclude risk events, arguably overlooked by the conventional approach, we presented the VUCA meter, intended to complement the conventional risk identification and assessment. The meter is based on the VUCA concept explained briefly later in this text, which stands for volatility, uncertainty, complexity, and ambiguity. The VUCA meter endeavors to investigate the VUCA’ility of the project. An example could be a search for items that pertain to the volatility of a particular project, the uncertainty, and so on. In short, the VUCA meter is designed as a normative method to capture risk factors with VUCA semantics as a point of view [6]. This research aims to test whether

the VUCA meter can improve the conventional risk identification process. It was done by selecting one large project currently under planning and testing the VUCA meter. Experts involved in the chosen project were divided into two workshops. Several focus questions were designed for each workshop. The purpose of the first workshop was to perform a risk identification and assessment based on the traditional framework presented in the PMI Standard for Risk Management in Portfolios, Programs, and Projects [8]. The purpose of the second workshop was to apply a new method for identifying and assessing risk based on the VUCA meter presented by Fridgeirsson and Ingason et al. [5]. The main focus of this study is to investigate whether the VUCA meter can supplement the conventional risk identification process by capturing Black Swan events in the domain of projects and project management. As the world is confronted with the enormous responsibilities related to, e.g., geopolitics, climate change, energy adaption, and social media, the isolation of risk that can harm sustainability seems imperative.

2. Literature Review

The importance of risk management in the context of project management has been widely discussed in the existing scientific literature [14,15]. All the tools and techniques used in risk management for projects are designed to help ensure that the project's delivered results are as expected and within identified constraints for the project. In the generic life cycle of projects, it is considered most effective when the risk events are identified and dealt with at an early stage of the project to be able to avoid big problems occurring in the project and to be aware of the risk events throughout its life cycle [7]. The risk management process is mainly divided into six steps: (1) Risk identification, where all possible risks that can have a negative impact on the project are identified; (2) risk assessment, including risk analysis, to determine which factors are the most important (riskiest) ones for the project; (3) a strategy and corresponding actions are developed and implemented to mitigate the risk; (4) monitoring and control of the risk; (5) report and integration against the risk; and (6) support for risk management, for example, with periodic project and risk meetings [16].

In this study, the emphasis is mainly on the beginning of the risk management process, the first two steps, where the risk events are identified and assessed. This is carried out using tools and techniques such as expert judgment, data gathering, data analysis, interpersonal and team skills, prompt lists, and meetings. Many of those involved in a project can contribute to the risk identification process, such as the project team members, customers, project manager, operations managers, stakeholders, end-users, and of course, the project risk specialist if assigned. Generally, the risk assessment is done by assessing on one hand the likelihood of a risk event occurring and on the other hand the impact of the same risk event on the project [17]. This conventional open approach to assess risk as described above has been disputed and there are several scientific research studies where it has been argued that this approach does not capture all the risk events that may affect the project, and significant risk events may be overlooked by using the conventional risk assessment techniques only [5,9,13,18]. That is because the likelihood of events to occur is one of the critical variables in the calculation when assessing the most significant risk events for the project. A case study from 2007 [9] discussed this systemic risk assessment. The authors argued that the most attention in the systemic risk assessment is devoted to the technical risk in projects, not other risk categories such as political risk, customer risk, partner and supplier risk, human risk, reputation risk, market, and financial risk.

In 2011, Geraldi, Maylor, and Williams published an article where they systematically reviewed the complexities of projects and pointed out that this is a key variable that impacts decisions in project management [19]. The type of complexity that is most frequently mentioned is structural complexity. Still, uncertainty is a relevant type of complexity and is one of the four concepts that constitute VUCA. The internal connection between complexity and risk was mentioned in the literature as early as in 1920 and has thus long been recognized [19]. In 2004, Linehan and Kavanagh defined projects as a confusing phenomenon that contain a lot of complexity and ambiguity, and the idea of a single clear

goal is not realistic [20]. Still, even though complexity is such a challenging concept to study in project management, it is only one of the four concepts that VUCA consists of. Nancy Green provided a passable description of the characteristics of a risk event that might surpass the conventional risk assessment procedure based on the work of Nassim Taleb see Table 1 [21].

Table 1. The criteria for a Black Swan event adapted from [21].

Emergency response to the problem and fixing the problem are different aspects.
A solution to the problem is unknown and must be created under dismal circumstances.
Public relations issues can be massive, putting pressure on reputation, credibility, and perception of the public.
Governmental and regulatory agencies may demand response.
Productivity and cash flow may be affected negatively, liquidity could become uncertain, and asset prices disturbed.
Despite the problem, the day-to-day operation must continue.

Although VUCA is often named in connection with risk in the literature, a normative risk identification process based on VUCA is not. However, a noteworthy study on VUCA and risk assessment is Szpitter and Sadkowska who recommend using a VUCA matrix “to identify and analyze project risks, thus filling the research gap relating to the lack of application of this tool in analyses in the area of project risk management” [22]. Other notable studies on risk are [23,24], connecting the VUCA era to supply sustainability management of supply chains.

The four components of VUCA are defined based on Bennett and Lemoine’s [6] discussions and definition in their article from 2014. Bennett and Lemoine define each part carefully, as well as how to address them, and give clear examples to explain the semantics of VUCA. The semantics of the Bennett and Lemoine study on the characteristics of VUCA provided the authors with means to develop the sections of the VUCA risk identification meter. Each section of the meter must be addressed individually since they require a unique response. The VUCA meter used in this study is accessible in Appendix A to the article.

3. The Case Study

The case chosen for this research is a large public infrastructure project with a long planning and deployment horizon. The project is highly strategical as it is a part of an urban planning policy to increase the effectiveness of a transport system and contribute to environmental sustainability. The project has complicated stakeholder and shareholder structure that includes several municipalities and the government. The project requires large financial investments with a public-private partnership arrangement required for parts of the project. In the case of a huge cost overrun, the consequences would have a significant impact on the national economy.

4. Methodology

In the selection of participants for this study, a convenience sample was used. A convenience sample is a nonprobability or non-random sampling where the sample is gathered using predefined criteria, which means that not everyone has an equal chance to participate in the research [25]. When workshops are used as a research method, they are designed to fulfil the purpose of the study and used as a tool to collect data about a certain subject [25]. Workshops are today a well-established arrangement whereby a group of people learn, acquire new knowledge, perform creative problem-solving, or innovate in relation to a domain-specific issue [26]. Two workshops were lined up for the study. The main goal of the workshops was to apply and compare two different approaches for identification of risk factors in the selected project: firstly, a conventional risk identification as presented by PMI, where the main risk factors are identified on the basis on given

focus questions and then rated on a scale for the likelihood of them occurring and the impact they would have; secondly, the VUCA risk identification method, where the main risk factors are identified based on five focus questions for each part of the term VUCA, 20 questions in total. In this case, the questions were composed based on the VUCA meter presented in the study by Fridgeirsson and Ingason et al. [5]. A group of ten experts working directly in the project preparation attended and were divided equally into two workshops. No one participated in both workshops and participants were instructed not to communicate regarding the workshops. The workshops were accurately planned and scheduled and were estimated to take around three hours each. Care was taken to make sure that the participants could prepare individually, so that the workshops would run as smoothly as possible. The questionnaire for the conventional risk identification was based on the traditional method presented in the PMI Standard for Risk Management in Portfolios, Programs, and Projects [8]. The questionnaire is divided into four focus questions and is answered by listing up factors that could be risky for the project related to each focus question. The focus questions are: (a) What risk events can impose operational risk? (b) What risk events can impose financial risk? (c) What risk events can impose legal and regulatory risk? and (d) What risk events can impose strategic risk?

In continuation, each risk factor is given value for the likelihood of occurring and for the impact, if it occurs. The values given for the likelihood and the impact are in the range of 1 to 5. The numbers indicate the following: (1) Very low, (2) Low, (3) Medium, (4) High, and (5) Very high.

The questionnaire developed for the VUCA risk identification is divided into four categories. Each category represents one of the four concepts VUCA consists of and each consist of five focus questions. These questions are as follows:

Volatility: (a) What complexity factors could lead to the need for many interfaces with other technologies, projects, or operations? (b) What volatility elements could lead to the need for more resources than expected? (c) What, from the perspective of volatility, could cause the project to take longer than planned? (d) What volatility factors could impact solid contract situation throughout the project timeline? (e) What volatility factors could cause the need for major changes in the objectives of the project?

Uncertainty: (a) What uncertainty factors could lead to the need for more information about technology components of the project? (b) What uncertainty factors could lead to the need for many stakeholders from different time zones? (c) What could cause the access to information to be limited due to uncertainty? (d) What uncertainty factors could impact well defined and approved scope? (e) What uncertainty factors could impact well-defined risk management?

Complexity: (a) What could lead to a complex political environment with many regulations to follow? (b) What complexity factors could lead to the need for many subcontractors, organizational departments, and cultural differences? (c) What complexity factors could lead to the need for many interfaces with other technologies, projects, or operations? (d) What are the factors of complexity making this a unique project not done before? (e) What complexity factors could make the decision-making not be straightforward?

Ambiguity: (a) What could cause the deliverables to not be as defined in the beginning due to ambiguity? (b) What ambiguity factors could cause the connections between tasks to become unclear? (c) What could lead to unexpected and unforeseen risk factors in an ambiguity environment? What could cause hidden agenda due to ambiguity? (e) What could lead to the need for unexpected/unknown stakeholders due to ambiguity? Brainstorming techniques were applied in both workshops and the individuals in the workgroups carefully facilitated. Pictures from the workshops can be found in Appendix B.

The data were analyzed in different ways, e.g., by using the multiplication rule of statistics to calculate the risk coefficient, the risk events were categorized, the range of the risk categories calculated, and even word clouds were prepared. However, these results are not the subject of the present study. The main objective of the study is to identify if the VUCA meter could identify “fat tail” risk events that would impact the

project. The result section is therefore mainly reporting on the application of the before-described characteristic of Black Swan events [21] to isolate such events from each of the two work groups.

Some risk factors were named in both workshops and therefore consequently removed from the list. The risk events identified in the respective workshops were then compared against the Black Swan criterions as defined by (E) in a two round Delphi technique survey using an adapted four-point Likert scale. The adaption involved removing the neutral option from the scale pressing the expert to decide the strength of the risk factor in context of the Black Swan attributes in Table 1. The expert panel consisted of students in the MPM (Master of Project Management) program at Reykjavik University. The MPM is a post graduate two-year course of studying project management. The MPM study line has been accredited by APM Association of Project Management and is approved by the Ministry of Education in Iceland. All students have training in project and risk management and experience from various industries. All students recognized the project under screening and were able to comprehend the complexities incurred. The expert panel contained 13 persons of both genders and an online tool was applied to conduct the Delphi two rounds.

5. Results

5.1. Workshops

The conventional method for risk identification delivered a total of 52 risk factors whereas 119 risk factors were obtained using the VUCA method, see Figure 1.

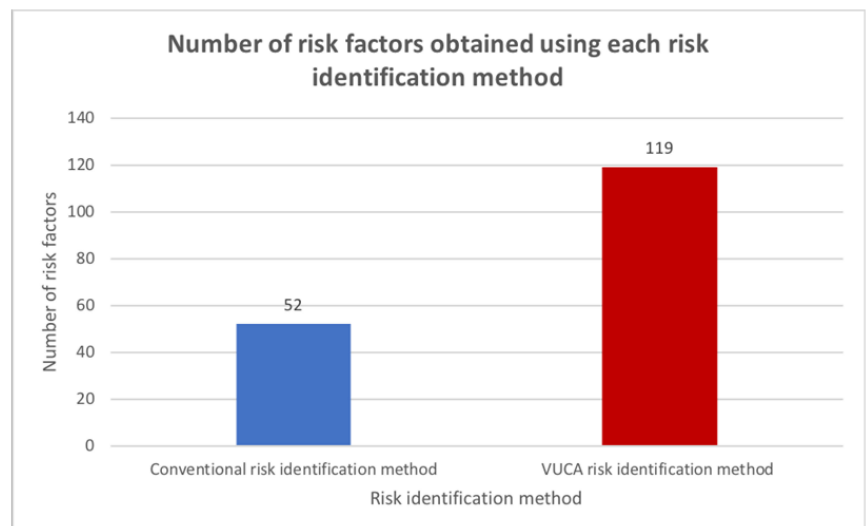


Figure 1. Number of risk factors obtained using each risk identification method.

A comparison of the risk factors obtained from each risk identification method shows that both methods captured risk factors that did not appear in the other method. The risk factors that only appeared when the traditional risk identification process was applied are shown in Table 2. The risk factors that were only captured by using the VUCA method are shown in Table 3. A large part of the risk factors identified were documented in both workshops, either in exactly the same form or with a different wording but the same meaning.

Table 2. Risk factors only captured using the conventional risk identification method.

Delays in other infrastructure (neighboring projects)
Overheating in the construction market
Failing to implement measures and incentives that will fulfil the project objectives
Currency fluctuation
Loss of reputation due to rights of construction personnel not followed
The new infrastructure will not give enough priority for the vehicles
Legal decision related to infrastructure, but operation is not catered for
Complicated interaction between design, planning, and EIA
The project not being able to bring expected urban qualities
Difficulties in getting good placing for a depot
Illegal size of fleet
Failures in branding the project will not draw new users
The project operation affected by delay in the system
Uncertainties in volumes calculations
Issues when obtaining land
Problems with EIA laws

Table 3. Risk factors only captured using the VUCA risk identification method.

Constantly needing reaffirming the ground/decision for the project
No ultimate decision maker that can give final answer
Decision on investment cost vs. maintenance cost (different budget)
Some part of the projects is forgotten/not delivered
The budget in manifesto will not be accepted every year by the government
The sponsor pushing towards downscaling to achieve more for the same budget
Change in key decision-makers
Complexities due to the current setup/ownerships of the project
Project scope is not clearly defined
Relatively short construction period per phase
Too much workload burns on the system
Facts are not clear enough for decision making
Uncertainty about who will run/operate part of the infrastructure
Major disruption during construction—affecting the construction time
Unexpected natural disasters, such as eruption, global warming, and climate
Complexities due to neighboring large project 1
Complexities due to neighboring large project 2
Not clear what is included in the project—not clear project definition
Ambiguity in toll discussion and policymaking
Responsibilities are not clearly defined
The municipalities pushing towards a larger scope—shifting the scope to manifesto
Timelines for different part of the project are not clear

Table 3. *Cont.*

Changes in direction at the operator
Different rhythm between organizations
Lack of commitment to the project PMO
Change of board members at the sponsor
Public vs. private cost
Mistakes in risk assessment
Pressure from construction development companies
Ambiguity in fleet type decision
Ambiguity in the ownership of the infrastructure
Human resource changes
An increase in inhabitants that is more than what was expected
Complex to integrate many modes of transport
The nature of the project and its linked to current situation and project in manifesto
Technical specification of solution unclear
Lack of interest
A financial crisis which results in higher costs of project components
Increased need to participate in dialog, public, media, and social
Expectation management
New transport/mobility solutions
Complex to phase the implementation of the route network
The size—large compared to Icelandic construction project
Things idealized/beautified
Unpredictable weather in Iceland
Unfavorable development of different fuel options
Market fluctuation
Population increase
Change in location of major workers/offices
New CO ₂ agreements—more reduction in emissions required

Another observation is worth mentioning. As mentioned in the literature review, Cirillo and Taleb [13] introduce the “tail risk” events as events that have much impact and shape our world, but are not likely to occur, and according to the authors are not as likely to be captured by using the conventional risk identification and assessment techniques. The risk factors having the lowest value for the likelihood of occurrence are all ranked in the range of 24 to 52 in the order of the risk coefficient obtained by the multiplication rule. The majority, or 70% of these risk factors, are ranked at 41 or later, which indicates that they are not considered very risky compared to the other risk factors. However, 60% of these risk factors have the value of impact in the range of 3.2 to 4. By comparing these low probability factors to the riskiest factors obtained by using the VUCA method, it can be seen that 60% of these risk factors would have been among the ten riskiest events in the VUCA risk assessment, by only taking the impact into consideration. The participants in the workshops were asked to rate the impact for each risk factor on the scale of 1 to 5. The participants in the workshop where conventional risk identification and assessment technique was used were also asked to rate the likelihood of occurrence for each risk factor. By getting this evaluation from the participants and viewing the average range in the answers from the participants from each workshop, it is possible to see the inconsistency

in their evaluation of the risk factors. The results showed that there was much more inconsistency in the evaluating of risk factors obtained when the conventional method was used than when the VUCA method was used. The average range was 2.32 for the impact and 2.31 for the likelihood when the conventional method was used but 1.55 for the evaluation of the impact when the VUCA method was used.

The inconsistency in the answers can be traced to the measuring instruments which are in this case the people participating in the research. The people can look at the same things in different ways and the understanding can be different. That can be traced to that they may not have the exact same background and may be working for different segments of the project and therefore, they have different point of view when evaluating.

Lastly, it should be noted that many of the risk events that are products of the workshops are generic and it is not easy to interpret them for the analysts and, in this case, the authors. This obscurity occurred despite care taken in advance preparation of the participants prior to the workshops. This indicates the need to improve the risk assessment process, e.g., by educating the risk assessors of the importance of phrasing exactly the context of the risk.

5.2. Delphi Surveys

For the first round of the Delphi survey, a cut-off point of >60% of the panelists either agreed or strongly agreed that the particular event is a Black Swan. The following list are the eight risk events from round no. 1 satisfying the >60% criteria. As can be detected from Tables 2 and 3, two of those events appeared in the conventional risk workshop and six appeared in the VUCA workshop.

- Overheating in the construction industry creates problems
- Legal decision related to infrastructure taken, but operation is not catered for
- The sponsor pushing towards down-scaling to achieve more for the same budget
- Major disruption during construction—affecting the construction time
- Unexpected natural disasters, such as eruption, global warming, and climate
- Changes in direction at the operator
- A financial crisis which results in higher costs of project component
- Unfavorable development of different fuel options

The second round included only the eight risk factors above. The cut-off point of >60% consensus among the panelists permitted the following risk factors as Black Swans.

- Overheating in the construction industry creates problems
- Major disruption during construction—affecting the construction time
- Unexpected natural disasters, such as eruption, global warming, and climate
- Changes in direction at the operator
- A financial crisis which results in higher costs of project component

One risk event is a product of the conventional workshop and four from the VUCA workshop.

6. Discussion

The study is based on preparing two kinds of risk identifications and assessments for the same project and executing this through two separate workshops with different sets of participants. We asked the question if the VUCA meter could augment the traditional risk identification practice by denoting risk events that may have been overlooked otherwise. The results are interesting and indicate that the assumption is valid. The findings can give an idea of the usefulness of the VUCA meter in terms of project risk identification.

By comparing the results from the VUCA risk identification method and the conventional risk identification method, it is evident that the number of risk factors identified by each method were different. The number of risk factors obtained by using the conventional method was 51 compared to 119 risk factors when using the VUCA method. This is a huge difference given that the time for both workshops was identical. The only difference

between the workshops was the work process; the approach that was used to elicit answers from the participants.

The conventional probabilistic and event-based approaches to risk assessment are great and have proven their usefulness. They do, however, have their limitations, especially when it comes to unprecedented events involving low-probability/high-impact risks, system risks, and risks that are less technical and more psychological/social in nature. Noteworthy is the study by Ackermann et al., who presented the “risk filter” that uses insights from forensics to identify risk exposure on future projects and tackle them [9]. Another study stating the difficulties of the conventional approach is by Qin et al. [27]. Titko et al. did an interesting study on how the escalation and severity of natural disasters will affect the public and need for new ways to approach the incurred risks [28]. Lastly, the authors would like to mention the cognitive theories of Amos Tversky and Daniel Kahneman on human limitations of decision making, see, e.g., [10,29]. The conventional method is an open approach relying on the experience and the cognitive state of mind of the participants. The VUCA meter is a normative approach that asks questions in a certain context. For the conventional workshops, five questions related to the conventional topics of a risk identification process were used to elicit risk factors, one at a time. In the VUCA workshops, 20 focus questions were used to elicit risk factors, five questions for each component part of VUCA. In this case, five focus questions were answered at a time. The results indicate that the VUCA method might be a better way to force people to think somewhat beyond the traditional framework used for identifying risk factors in a project. The traditional framework included operational, financial, legal and regulatory, and strategic risk, but projects in modern times are faced with risk that is not necessarily encapsulated by this framework. Furthermore, the VUCA method may help to bypass cognitive biases that are well known sources for risk, see, e.g., the landmark studies of Daniel Kahneman and Amos Tversky [10]. The risk factors that were captured using the VUCA method but not with the conventional method were of different kinds. Still, most of them seem to be related to the social and the environmental part of the project. This is the outcome of a framework that directed the participants to think of risk factors that occur as a result of the time of volatility, uncertainty, complexity, and ambiguity.

7. Conclusions

The authors have confidence in that the VUCA meter can be developed further and provide risk managers with a valuable tool to capture risk factors that would be undetected by a conventional method. It could also be interesting to take this research further. Future studies should select more than one project from different sectors in order to assess if this VUCA method works differently in different sectors. Subsequently, it would be interesting to develop a method which is a combination of the two methods and try this new method to identify and assess potential risk factors for projects. The outcome will be some kind of improved version of the existing conventional method currently in place to identify and assess project risk. Lastly, a study based on the present study with improved VUCA semantics and an improved process to ensure a clear context of the risk events is likely to provide even better results. It is also worth mentioning that the authors have now, in light of the results and observations of this study, issued a new version of the VUCA meter. The new version comes with more comprehensive semantics and vocabulary. Moreover, an exact template on the work procedure has been devised. This is a process leading the facilitator and the team of analyst in steps toward a solution.

Author Contributions: T.V.F. led the study and arranged the paper in the present conceptualization form. He also supervised the research, designed the Delphi surveys, and facilitated the workshops. H.T.I. supervised the research and contributed to the management of the workshops, surveys, and writing. A.Y.G. was the main researcher in the initial investigation and contributed to writing. S.H.B. contributed to writing, review, and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki and approved in accordance with the requirements of the Institutional Review Department of Reykjavik University (RU-MPM-Review-Board-May 2020, 1 May 2019).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: Authors declare that no conflict of interest is connected to this study.

Appendix A. The VUCA Meter

Criteria	Compliance Weights					Avg. Score	Statement Score Range
	1	2	3	4	5		
Volatility	1	2	3	4	5		
Simple in planning (straightforward/sequential execution)							
Resource needs are known and accessible							
Adequate timeframe with good slack in schedule							
Solid contracts throughout project duration							
Known, well defined objectives							
Average score:							
Project score range:							
Uncertainty	1	2	3	4	5		
Uses few and proven technology components							
Stakeholders are few, with few time zones/cultural differences							
Information is easy to obtain							
Scope is well defined and approved							
Risk management is well defined							
Average score:							
Project score range:							
Complexity	1	2	3	4	5		
Few and simple regulatory or political environments							
Few subcontractors, organizational departments, and cultural differences							
Few interfaces with other technologies, projects or operations							
Has been done many times before							
Clear governance, straightforward decision-making							
Average score:							
Project score range:							
Ambiguity	1	2	3	4	5		
Deliverables are well defined, no "unknowns unknowns"							
Connections between tasks are clear							

Criteria	Compliance Weights					Avg. Score	Statement Score Range
Risk factors are well known and documented							
No “hidden agenda”							
All stakeholders and their relationship are recognized							
Average score:							
Project score range:							

Appendix B. Pictures from the Workshops

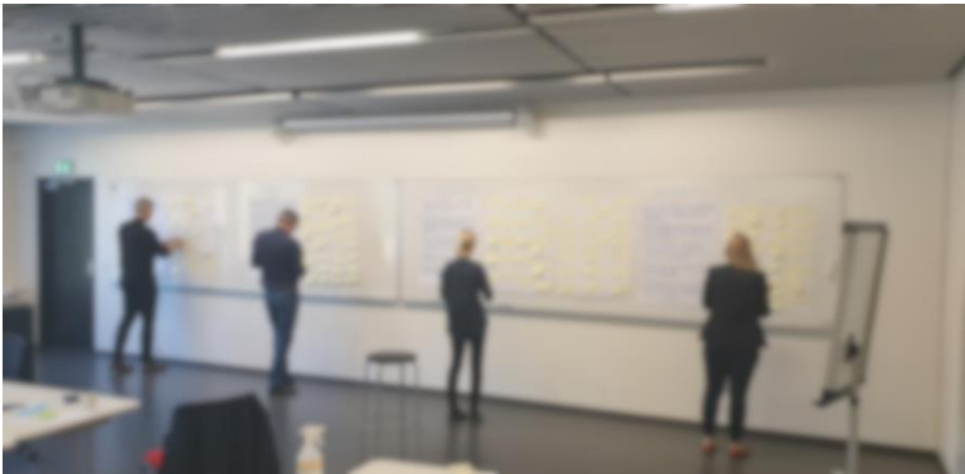


Figure A1. The conventional risk identification workshop. Photo taken on site by the authors.



Figure A2. The VUCA risk identification workshops. Photo taken on site by the authors.

References

1. Vaðlaheiðarganga, Saga. Available online: <https://www.vadlaheidi.is/is/sagan> (accessed on 18 October 2021).
2. Heidarson, J.T. Vaðlaheiðargöng—Mat á Þjóðhagslegri Arðsemi, January 2006. Available online: https://www.rha.is/static/files/Rannsóknir/2006/Skyrsla_loka.pdf (accessed on 18 October 2021).
3. Kjarninn. Available online: <https://kjarninn.is/frettir/2018-03-12-let-reikna-kostnad-vid-vadlaheidargong-i-samraemi-vid-log-um-rikisabyrgdir/> (accessed on 18 October 2021).
4. DV. Available online: <https://www.dv.is/frettir/2019/07/15/tekjur-vadlaheidarganga-65-70-minni-en-aaetlad-var> (accessed on 18 October 2021).
5. Fridgeirsson, T.; Ingason, H.; Jonasson, H.; Kristjansdottir, B. The VUCAity of Projects: A New Approach to Assess a Project Risk in a Complex World. *Sustainability* **2021**, *13*, 3808. [CrossRef]
6. Bennett, N.; Lemoine, G.J. What a difference a word makes: Understanding threats to performance in a VUCA world. *Bus. Horiz.* **2014**, *57*, 311–317. [CrossRef]
7. Thamhain, H. Managing Risks in Complex Projects. *Proj. Manag. J.* **2013**, *44*, 20–35. [CrossRef]
8. PMI. *Project Management Institute, The Standard for Risk Management in Portfolios, Programs, and Projects*; PMI: Newtown Square, PA, USA, 2019.
9. Ackermann, F.; Eden, C.; Williams, T.; Howick, S. Systemic risk assessment: A case study. *J. Oper. Res. Soc.* **2007**, *58*, 39–51. [CrossRef]
10. Kahneman, D.; Tversky, A. Prospect Theory: An Analysis of Decision under Risk. *Econometrica* **1979**, *47*, 263–291. [CrossRef]
11. Flyvbjerg, B.; Glenting, C.; Rønne, A. *Procedures for Dealing with Optimism Bias in Transport Planning*; The British Department for Transport, Guidance Document: London, UK, 2004.
12. *The Black Swan: The Impact of the Highly Improbable: With a New Section: “On Robustness and Fragility” (Incerto) Paperback—11 May*, 2nd ed.; Random House Publishing Group: New York, NY, USA, 2007.
13. Cirillo, P.; Taleb, N.N. Tail risk of contagious diseases. *Nat. Phys.* **2020**, *16*, 606–613. [CrossRef]
14. Ward, S.C.; Chapman, C.B. Risk-management perspective on the project lifecycle. *Int. J. Proj. Manag.* **1995**, *13*, 145–149. [CrossRef]
15. Morris, P.W.G.; Pinto, J.; Söderlund, J. *Introduction: Towards the Third Wave of Project Management*; Oxford University Press: Oxford, UK, 2011.
16. Rodrigues-Da-Silva, L.H.; Crispim, J. The Project Risk Management Process, a Preliminary Study. *Procedia Technol.* **2014**, *16*, 943–949. [CrossRef]
17. PMI. *Foundational Standards*; PMI: Newtown Square, PA, USA, 2017.
18. Nieto-Morote, A.; Ruz-Vila, F. A fuzzy approach to construction project risk assessment. *Int. J. Proj. Manag.* **2011**, *29*, 220–231. [CrossRef]
19. Gerald, J.; Maylor, H.; Williams, T. Now, let’s make it really complex (complicated). *Int. J. Oper. Prod. Manag.* **2011**, *31*, 966–990. [CrossRef]
20. Linehan, C.; Kavanagh, D. *From Project Ontologies to Communities of Virtue*; Department of Management & Marketing University College Cork, National University of Ireland: Cork, Ireland, 2004.
21. Green, N. Keys to Success in Managing a Black Swan Event [White Paper], AON Corporation. Available online: http://www.aon.com/attachments/risk-services/Manage_Black_Swan_Event_Whitepaper_31811.pdf (accessed on 9 October 2021).
22. Szpitter, A.; Sadowska, J. Using VUCA matrix for the assessment of project environment risk. *Zarządzanie Finans.* **2016**, *14*, 401–413.
23. Ocicka, B.; Jolanta, T. “Supply Chain Sustainability Risk Management in a Digitally VUCA Changing World”. In *The Economics of Sustainable Transformation*; Routledge: New York, NY, USA, 2021; pp. 167–190.
24. Gao, Y.; Feng, Z.; Zhang, S. Managing supply chain resilience in the era of VUCA. *Front. Eng. Manag.* **2021**, *8*, 465–470. [CrossRef]
25. Etikan, I.; Musa, S.A.; Alkassim, R.S. Comparison of Convenience Sampling and Purposive Sampling. *Am. J. Theor. Appl. Stat.* **2016**, *5*, 1–4. [CrossRef]
26. Ørngreen, R.; Levinsen, K. “Workshops as a Research Methodology”. *Electron. J. E-Learn.* **2017**, *15*, 70–81.
27. Qin, J.; Xi, Y.; Witold, P. Failure mode and effects analysis (FMEA) for risk assessment based on interval type-2 fuzzy evidential reasoning method. *Appl. Soft Comput.* **2020**, *89*, 106134. [CrossRef]
28. Titko, M.; Ristvej, J.; Zamiar, Z. Population preparedness for disasters and extreme weather events as a predictor of building a resilient society: The Slovak Republic. *Int. J. Environ. Res. Public Health* **2021**, *18*, 2311. [CrossRef] [PubMed]
29. Kahneman, D. *Thinking, Fast and Slow*; Macmillan: New York, NY, USA, 2011.



Department of Engineering

Reykjavík University

Menntavegur 1

101 Reykjavík, Iceland

Tel. +354 599 6200

Fax +354 599 6201

www.ru.is