UiT The Arctic University of Norway

Faculty of Science and Technology

Operationalising Critical Infrastructure Resilience

From Assessment to Management

Bjarte Rød

A dissertation for the degree of Philosophiae Doctor – May 2020

Operationalising Critical Infrastructure Resilience

From Assessment to Management

By

Bjarte Rød

Thesis submitted in fulfilment of the requirements for the degree of

Philosophiae Doctor (PhD)

UiT The Arctic University of Norway

Faculty of Science and Technology

Department of Technology and Safety

~In memory of my father

Preface and acknowledgements

The long road towards this dissertation began in August 2015, when I started my academic career at UiT The Arctic University of Norway, Department of Technology and Safety. As I now submit this thesis, I would like to show my appreciation to everyone that have made this possible.

This work has been carried out in collaboration with my supervisors, Prof. Abbas Barabadi and Prof. Christer Pursiainen. I wish to thank them for the guidance and encouragement, and for sharing their valuable knowledge throughout this project. A special thanks to Christer for taking me on board and introducing me to the field of societal safety and security through the IMPROVER project. You have always supported me, challenged me, and given me responsibility.

Most of this research has been carried out in association with the European Union research project IMPROVER (2015-2018), funded from the Horizon 2020 Research and Innovation Programme under grant agreement no. 653390. I look back at the time in the IMPROVER project with joy and appreciation. It was a real pleasure to work in such a multi- and interdisciplinary environment, participating in meetings and workshops all over Europe. I wish to thank all the partners, associated partners, operators, and other stakeholders in the project. A warm thanks to Dr. David Lange for his coordinating efforts and for valuable contributions to our joint publications. I also would like to thank Gonçalo Cadete for sharing his interesting and innovative perspectives during the many Skype meetings with David. Furthermore, I show my appreciation to Dr. Marianthi Theocharidou for hosting me during my visit at the European Commission's Joint Research Centre in Ispra, Italy, in the spring of 2018.

Through seminars and workshops, I was lucky to establish a strong cooperation with Assoc. Prof. Jonas Johansson at Lund University, Sweden. I wish to thank him for all the help and for proving me with invaluable insights, and for the hospitality during my several visits in Lund.

I would like to thank the Norwegian Water Norwegian Water Resources and Energy Directorate for giving me access to data and for contributing with comments and ideas in one of my case studies. I also would like to recognize Assoc. Prof. Yonas Ayele at Østfold University College (former postdoctoral researcher at UiT) for helping me in the data collection and extraction process. In the same study, I wish to thank Assoc. Prof. Masoud Naseri for his contributions with respect to the data analysis and the writing process. I am also very grateful for the friendship we have established along the way.

I am thankful for all the support from all other friends and colleagues at the Department of Technology and Safety, including Brian, Are, Reidar, Svein, Maria, Lise, Johana, Jens Andreas, Rezgar, Eirik, Bengt, and many more. Moreover, I would like to thank the leadership and administration at the department for assistance during the project, led by Yngve Birkelund and the always-positive Gunn-Helene Turi.

I would like to express my gratitude to my friends and family for support and encouragement over all these years. A special thanks to my brother Tore, and my dear mother.

Last, I would like to thank Lene, my becoming wife, for all her love and support. This would not be possible without you.

Bjarte Rød

Tromsø, Norway
May 2020

Abstract

Over recent decades, it has been evident that society relies heavily on critical infrastructures (CIs) to provide and maintain vital societal functions, such as water, electricity and transportation. Traditionally, in order to ensure the delivery of such functions, the focus has been on protecting the infrastructures' systems from adverse and extreme events. However, large-scale events, such as hurricanes, floods, cyberattacks and the ongoing coronavirus pandemic, illustrate that is not always feasible to protect infrastructures from all types of threats; it can be technologically impossible and extremely costly. Hence, the concept of critical infrastructure resilience (CIR) has been introduced, in order to enable CIs and their surrounding organisations to bounce back and cope with surprises and high-consequence events. CIR has been the subject of vibrant scholarly discussion for over a decade. Yet there is no consensus on some fundamental questions, most importantly on how CIR could be measured, analysed, evaluated, and enhanced. In other words, a proper approach to CIR management is missing. The aim of this thesis is to solve this challenge.

From a theoretical and practical perspective, I review current literature and practices, to explore and justify the need and objectives for operationalising CIR and, thus, improve the understanding of the application and interaction of different resilience concepts. Moreover, methodologically, I review scientific literature, constituting state of the art in real-life application to CIs. I further proceed, through demonstration, evaluation and implementation in a real-life environment, to develop new methods and techniques for CIR assessments. Finally, to facilitate the operationalisation of CIR, based on the feedback from operators through the implementation and demonstration, I develop an overall CIR management framework that is compatible with a variety of CIR assessment techniques, which can be integrated into existing risk management practices.

The results of this study show that the CIR concept goes beyond traditional risk management and covers more than pre-event capabilities, acknowledging that protection of CIs can never be guaranteed. Based on the results from the demonstration, evaluation, and implementation of resilience assessment techniques and methods, I defend the plurality of techniques and methods, emphasising the need for measurability and comparability. Currently, there is no single approach, method or technique that would provide all the answers for all sectors, conditions, situations, needs or resources for a CI risk and resilience assessment. In addition, the latter part of a CI resilience assessment – namely, how to evaluate the results and compare them against public tolerance levels – seems to be largely underdeveloped. The study shows that research regarding CI resilience of real-life infrastructures, and especially towards how to enhance CI resilience, is still in its infancy, where substantial efforts are needed towards drawing informed conclusions with respect to their level of resilience and the effect of interdependencies.

The structures and processes of the proposed CIR management framework are proved to effectively facilitate the plurality of assessment techniques and methods, helping to conceptualise, operationalise and methodologically enhance CIR. The framework utilises the often-used practices of risk management, thus modifying the current international management standard towards that of CIR management. To this end, I present a framework that closely follows the standard risk management typology, but adapted to CIR.

For successful CIR management, I conclude with five maxims: no duplicate practices; tailorability and plurality of assessment techniques and methods; measurability; and relative ease of use.

Keywords: critical infrastructure; resilience; real-life; case studies; organizational resilience; technological resilience; risk management; ISO 31000; resilience management; resilience assessment; recoverability; operationalisation.

List of appended papers

Paper I **Rød, B.,** Barabadi, A., and Gudmestad, O.T. (2016). Characteristics of arctic infrastructure resilience: Application of expert judgement. *Proceedings of the Twenty-sixth (2016) International Ocean and Polar Engineering Conference (*pp. 1226 – 1233*).* Rhodes, Greece, June 26-July 1, 2016. ISBN 978-1-880653-88-3; ISSN 1098-6189.

Paper II Pursiainen, C., **Rød, B.,** Baker, G., Honfi, D., and Lange, D. (2017). Critical Infrastructure Resilience Index. In Walls, Revie & Bedford (Eds.), *Risk, Reliability and Safety: Innovating Theory and Practice. Proceedings of the 26th European Safety and Reliability conference, ESREL* (pp. 2183 – 2189). Glasgow, Scotland, September 25-19, 2016. London, UK: Taylor & Francis Group. ISBN 978-1-138-02997-2.

Paper III **Rød, B.,** Pursiainen, C., Reitan, N.K., Storesund, K., Lange, D., and Mira da Silva, M. (2018). Evaluation of resilience assessment methodologies. In M. Cepin & R. Bris (Eds.), *Safety and Reliability – Theory and Applications. Proceedings of the 27th European Safety and Reliability Conference, ESREL* (pp. 1039 - 1051). June 18-22, 2017, Portoroz, Slovenia. London, UK: Taylor & Francis Group. ISBN 978-1138629370.

Paper IV Storesund, K., Reitan, N. K., Sjøstrøm, J., **Rød, B.,** Guay, F., Almeida, R., Theocharidou, M. (2018). Novel methodologies for analysing critical infrastructure resilience. In Haugen et al. (Eds.), *Safety and Reliability – Safe Societies in a Changing World. Proceedings of the 28th European Safety and Reliability Conference, ESREL* (pp. 1221 – 1229). London, UK: Taylor & Francis Group. ISBN 978-0-8153-8682-7.

Paper V **Rød, B.,** Lange, D., Theocharidou, M., and Pursiainen, C. (2020). From risk management to resilience management in critical infrastructure. *Journal of Management in Engineering,* 36(4): 04020039. DOI: 10.1061/(ASCE)ME.1943-5479.0000795.

Paper VI **Rød, B.,** Barabadi, A., and Naseri, M. (Forthcoming 2020). Recoverability modelling of power distribution networks using accelerated life models: The case of power cut due to extreme weather events in Norway. Manuscript accepted for publication in *Journal of Management in Engineering.* DOI: 10.1061/(ASCE)ME.1943-5479.0000823.
Article published online on July 9, 2020. Printed version to be published in Volume 36 Issue 5 – September 2020

Paper VII **Rød, B.,** and Johansson, J. Critical Infrastructures: How resilient are they? Manuscript to be submitted for possible publication in an international journal.
Revised version of the manuscript submitted to Reliability Engineering & System Safety on July 8, 2020.

List of publications not included in the thesis

Papers in conference proceedings

Rød, B., Barabadi, A., Ayele, Y. Z., Lange, D., Honfi, D., and Droguett, E.Z. (2017). Probabilistic metric of infrastructure resilience considering time-dependent and time-independent covariates. In M. Cepin & R. Bris (Eds.), *Safety and Reliability – Theory and Applications. Proceedings of the 27th European Safety and Reliability Conference, ESREL* (pp. 1053 - 1060). June 18-22, 2017, Portoroz, Slovenia. London, UK: Taylor & Francis Group. ISBN 978-1138629370.

Cadete, G., **Rød, B.,** and Mira da Silva, M. Implementation guidance for resilience management of critical infrastructure. (2018). In Haugen et al. (Eds), *Safety and Reliability – Safe Societies in a Changing World. Proceedings of the 28th European Safety and Reliability Conference, ESREL* (pp. 1923 – 1931). London, UK: Taylor & Francis Group. ISBN 978-0-8153-8682-7.

Pursiainen, C., **Rød, B.** Evaluation of maintenance as a resilience indicator. Paper presented at ICEFA VII: Seventh International Conference on Engineering Failure Analysis, 3-7 July, 2016.

Honfi, D., Lange, D., Pursiainen, C., and **Rød, B.** On the contribution of technological concepts to the resilience of bridges as critical infrastructure assets. In *19th IABSE Congress Stockholm 2016: Challenges in Design and Construction of an Innovative and Sustainable Built Environment* (pp. 975 – 982). 21 – 23 September, 2016, Stockholm, Sweden. Zurich, Switzerland: International Association for Bridge and Structural Engineering (IABSE). ISBN 9783857481444

IMPROVER project publications*

Deliverable	Year	Title
Deliverable 1.1.	2016	International survey
Deliverable 1.4	2016	Report of operator workshop 1
Deliverable 1.6	2018	Report of operator workshop 3
Deliverable 2.2	2016	Report of criteria for evaluating resilience
Deliverable 2.3	2016	Evaluation of resilience concepts applied to critical infrastructure using existing methodologies
Deliverable 3.2	2017	Technological resilience concepts applied to critical infrastructures
Deliverable 5.1	2017	Framework for implementation of resilience concepts to critical Infrastructure
Deliverable 6.2	2018	Workshop report following demonstration of the methodology
Deliverable 6.3	2018	Report of critical evaluation of the methodology applied to critical infrastructure
Deliverable 7.6	2018	Operationalisation of resilience to critical infrastructure

*Contributing to deliverables related to the European Union research project IMPROVER (2015-2018), funded from the Horizon 2020 Research and Innovation Programme under grant agreement no. 653390. Available from http://improverproject.eu/category/results/.

Abbreviations and notations

AFT	Accelerated Failure Time
ANSI	American National Standards Institute
ASIS	American Society for Industrial Security
BRT	Benchmark Resilience Tool
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIR	Critical Infrastructure Resilience
CIRE	(Guidelines for) Critical Infrastructure Resilience Evaluation
CIRI	Critical Infrastructure Resilience Index
CIs	Critical Infrastructures
DSB	The Norwegian Directorate for Civil Protection (Direktorat for Samfunnssikkerhet og Beredskap)
DSRM	Design Science Research Methodology
EEA	The European Economic Area
EPCIP	European Programme for Critical Infrastructure Protection
EU	The European Union
ICI-REF	The IMPROVER Critical Infrastructure Resilience Framework
IORA	IMPROVER Organisational Resilience Analysis
ISO	International Organization for Standardization
ITRA	IMPROVER Technological Resilience Analysis
NIAC	National Infrastructure Advisory Council
NRA	National Risk Assessment
NVE	The Norwegian Water Resources and Energy Directorate (Norges Vassdrag- og Energidirektorat)
OECD	Organisation for Economic Co-operation and Development
PHM	Prognostics and health management
RM	Risk Management
TLR	Technological Readiness Level
UNISDR / UNDRR	United Nations Office for Disaster Risk Reduction

f	Failure mechanism
Q_r	Residual performance
r	Restoration process

R_j	Reliability of infrastructure
S_{Ci}	Score of how well the methodology fulfils the criteria *i*
t	Time
w_i	Weighting, represents the importance of each of the criteria *i* in achieving the desired results
$X_{i,j}$	The assessment of how well the different methodologies fulfil the criteria *i* in the evaluation *j*
Λ_j	The product of organisational resilience, maintainability, PHM efficiency, and supportability
$\Psi j\,(t)$	Resilience at time *t*

Table of Contents

List of Tables

List of Figures

Part I: Thesis summary

1 Introduction

Modern society is reliant on highly interconnected infrastructures providing critical services: so-called critical infrastructures (Moteff, 2010). In the European Directive from 2008 (The Council of the European Union, 2008) a critical infrastructure (CI) is defined as follows:

> *An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.* (p. 3)

As the definition emphasises, the loss of function of a CI – such as supply of water and electricity – can potentially lead to severe consequences for society. As a natural consequence of the technological developments over recent decades, CIs have become more and more interconnected (Johansson & Hassel, 2010). This allows for an easier and faster exchange of services of various forms (Organisation for Economic Co-operation and Development (OECD), 2011), but it has a downside attached to it. Infrastructure, people and economic interest interact and create both vulnerabilities and opportunities. Failure in a CI can potentially lead to loss of functionality in other key functions in society (Kotzanikolaou, Theoharidou, & Gritzalis, 2011). Large-scale events – such as the Argentina, Paraguay and Uruguay black-out in 2019, Hurricane Sandy in 2012, Hurricane Dagmar in Norway in 2011, the Eyjafjallajökull eruption in 2010, the European black out in 2006, and the ongoing Coronavirus pandemic illustrate the complexities and interdependencies involved, causing cross-border impacts. These events also reveal that it is very difficult, and often not feasible, to protect CI systems from all kinds of possible threats and hazards. For example, climate change induces more frequent and extreme weather events (Field, Barros, Stocker, & Dahe, 2012), which can be unpredictable and, hence, hard to find suitable predictive measures against. Over the course of the past decades, economic losses from natural disasters have increased significantly, from $528 billion (1981 – 1990), $1,197 billion (1991 – 2000) to $1,213 billion over the period 2001 – 2010 (Munich Re, 2012). In the last period, hurricanes and the resulting storm surges caused the highest economic losses. Moreover, with the changing global threat picture, CIs have also become targets for malicious attacks, both physically and in the cyber domain. As the World Economic Forum (2017, p. 7) highlights, technology is changing physical infrastructures:

"Greater interdependence among different infrastructure networks is increasing the scope of systemic failures – whether from cyberattacks, software glitches, natural disasters or other causes – to cascade across networks and affect society in unanticipated ways". For instance, in 2015, the Ukraine power grid experienced a cyber-attack from a foreign state, affecting 225, 000 people (Liang, Weller, Zhao, Luo, & Dong, 2016), illustrating the vulnerabilities new technologies bring. In Norway, the Norwegian Police Security Service (PST) (2020) lists sabotage of CIs as one of the top three threats in 2020 in Norway, underlining that so-called hybrid threats to CIs are emerging.

Therefore, a central question raised in the societal safety and security discourse is how to minimise the impact of such events. Traditionally, the common strategy has been to protect CIs, in order to reduce risks. However, the characteristics of large-scale crisis are often unpredictable in nature and initiated by low probability events or sequences of events. Consequently, such events rarely unfold the way we expect them to, and protecting infrastructures against all types of threats is not feasible; it is technologically impossible and extremely costly. Hence, we should design CIs that have the ability to bounce back, in order to cope with surprises and high-consequence events.

Recently, to solve this problem, the concept of resilience has grown in this field, acknowledging the need for resilient infrastructures and societies – having the ability to bounce back from extreme events. Adding to the risk management practices in CIs, Critical Infrastructure Resilience (CIR) has been a subject of vibrant scholarly discussion for over a decade (e.g. Luiijf, Nieuwenhuijs, Klaver, van Eeten, & Cruz, 2008; Petit, Wallace, & Philips, 2014; Pursiainen, 2018; Pursiainen & Gattinesi, 2014). Yet, as my study shows, there is no consensus on some fundamental questions, most essentially on how CIR should be measured, assessed and duly enhanced. This situation has hindered the development of the concept into a practical tool that could be operationalised by the CI operators. My claim therefore is that there is a need for a proper CIR management approach that could be incorporated into existing risk management practices. To that effect, in this thesis, I strongly defend the CIR approach and present methodologies to solve the above challenge. I argue that this can be done in ways that are relatively easy to incorporate into the practices of operators, complementing their existing practices rather than duplicating or replacing them. I wish to contribute to both conceptual and the methodological discussion in the field with new insights.

1.1 Background

While the definition of a CI is quite easy to perceive and understand, the definition of resilience is contested and leaves greater room for subjectivity. Resilience as a concept is not something completely new, but a common understanding of what resilience is across sectors and academic fields seems to be lacking (see e.g. Bergström, Van Winsen, & Henriqson, 2015; Bhamra, Dani, & Burnard, 2011; Hosseini, Barker, & Ramirez-Marquez, 2016; Patriarca, Bergström, Di Gravio, & Costantino, 2018). There are many definitions originated from different domains, such as engineering resilience (e.g. Righi, Saurin, & Wachs, 2015), organisational resilience (e.g. Burnard & Bhamra, 2011), and psychological resilience (e.g. Fletcher & Sarkar, 2013), reflecting the needs and objectives of the concept as relevant to themselves. The original meaning of the word stems from the Latin word 'resiliere', which means to bounce or spring back (Manyena, O'Brien, O'Keefe, & Rose, 2011) and it was first

introduced in the textile and metal industries to express the elasticity of materials. However, in the field of safety and security resilience, it was in the early 2000s that the concept started to make its way into the discourse (Bergström et al., 2015). A common way of describing resilience, first introduced by Bruneau et al. (2003), is the famous resilience triangle, illustrating the loss of performance of a system. A simplistic presentation of the performance of a given system is illustrated in Figure 1. The figure shows the loss of functionality from damage and disruption, as well as the pattern of restoration and recovery over time after a certain loss. At time t_i, the system develops a failure mechanism, *f*, and the residual performance (Q_r) is reduced until t_f. This is followed by a restoration process, *r*, ending at t_r. Before the incident occurs, the system suffers a smaller reduction in performance due to normal tear and wear. After a successful recovery process, the same process is repeated.

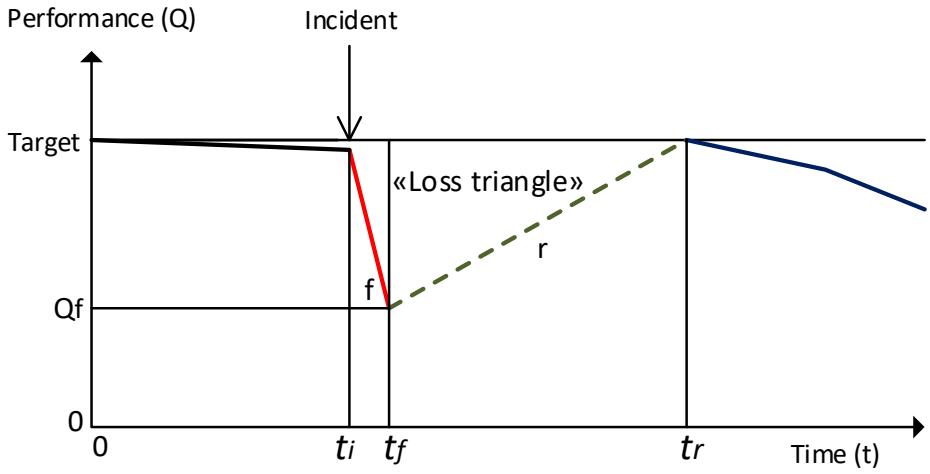

Figure 1. The resilience triangle. Adapted from Lange et al. (2017)

Following this presentation of resilience, there is a certain temporal dimension to resilience (Lange et al., 2017), covering the phases before, during and after an event. This is also consistent with the resilience definition provided by the United Nations Office for Disaster Reduction (UNDRR, formerly UNISDR). Resilience is defined as follows:

> *The ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management.* (UNISDR, n.d.)

As the definition emphasises, several strategies in conjunction can make a system resilient, from mere protection to adaptation and recovery. If we again consider the performance loss function introduced in Figure 1, but also now adding the performance of two other systems in Figure 2, curves B and C represent the two other systems. Let us say that the curves represent different resilience strategies through which organisations deal with hazards and the respective investment in the different temporal dimensions of CIR. The initial system (A) is not only less resistant but, when broken, it plummets and recovers slowly. System C is resistant but finally collapses altogether. System B's resilience curve resembles the idea of the resilience triangle. The fundamental idea is that reducing the triangle in all its dimensions would increase resilience, inheriting several temporal abilities.

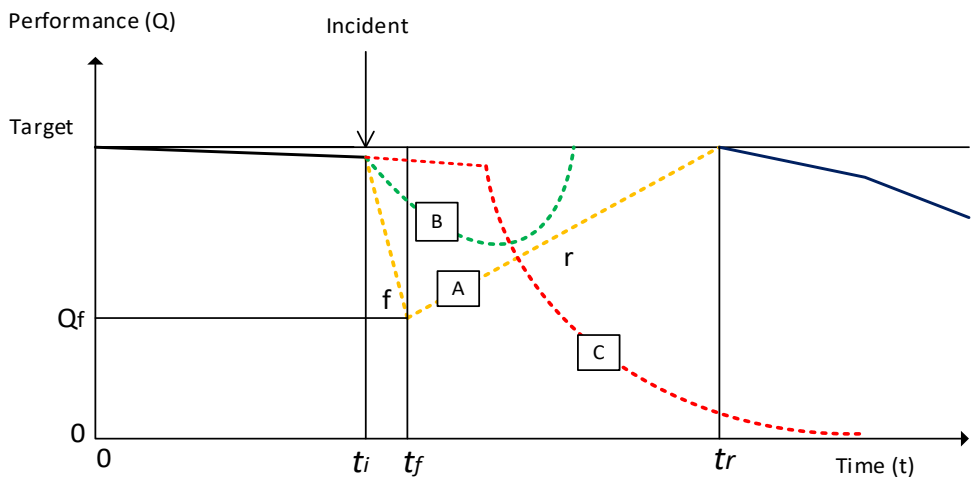

Figure 2. The 'resilience curve' for three different systems

At policy level, the protection strategy has been the traditional CI approach. In 2008, the European Union (EU) adopted the Directive on the identification and designation of European Critical Infrastructure with the intention to improve their protection (The Council of the European Union, 2008). The European Programme for Critical Infrastructure Protection (EPCIP) later implemented the directive. Hence, the aim was to protect infrastructure from threats and hazards, which is closely linked to the concept of resistance and robustness. In 2013, after the first evaluation of EPCIP (European Commission, 2013), and remaining in the 2019 evaluation report (European Commission, 2019), two main issues were brought up: how to handle CI interdependencies and how to enhance CI resilience. The latter indicates that protection is not necessarily sufficient, emphasising the need for additional abilities and capacities, such as absorption, adaption and recovery. In 2010, in parallel with this process, the European Commission initiated the process of making national risk assessment (NRA) guidelines, forming the basis for Member States' individual risk assessments. The aim of such assessments is to identify, analyse and evaluate the most important disaster risks that the European nations (EU/EEA) face. Most of the national risk assessments address loss of functionality in CI as a potential hazard. However, this is often only addressed as the consequence of some other hazard or threat. Moreover, as pointed out by the European Commission (2017), the CI operators' own risk assessments are often not included at the regional, national and cross-border levels. This has raised the need for better inclusion of CI data in national risk assessments and for the operationalisation of CIR as an umbrella concept to cover all stages of crisis management, complementing the traditional risk management approach.

Despite not being an EU member, Norway as a part of the European Economic Area (EEA) has adopted many of the same strategies and policies. From 2011, the Norwegian Directorate for Civil Protection (DSB) has carried out national risk assessments, following the same guidelines and principles as its neighbouring EU countries (IMPROVER Project, 2016b). The national risk assessment report from 2013, later updated in 2014, emphasises the need for 'resilient societies', "stressing that due to complex relationships and mutual interdependencies in society, resilience may become of greater strategic importance in the future in terms of efforts to strengthen society" (Pursiainen, 2018, p.635).

Consequently, with the shift in policy, resilience has become an emerging concept in the scientific world, across several dimensions and domains. Safety and security is a multi- and interdisciplinary field, which is clearly illustrated when it comes to CIR, including the technological, engineering, organisational, societal and economic domains. Thus, it can be difficult to find suitable ways to operationalise the concept. However, if the ultimate goal is to enable CIs, as socio-technical systems, to resist, absorb and recover from unwanted events, I contend that it is crucial to find ways to measure and assess resilience, in order to enhance it. Over the past 10-15 years, numerous ways to analyse resilience have been developed, encompassed in resilience assessment methodologies and frameworks, using different methods and techniques. Since I started this project in 2015, the development has experienced an exponential growth in academic production. As my scoping study shows, over the course of my project (2015-2020), as many as 265 research articles have tried to achieve this. Yet there are no commonly accepted metrics for CIR available, and few of them have been operationalised in a real-life environment. In the technological and engineering domain, resilience refers to the physical structures themselves of CIs, focusing on their ability to resist damage and minimise the loss of function during a disruption. Here, there are numerous different assessment techniques and frameworks, most often quantitative (see e.g. Hosseini et al., 2016; Liu & Song, 2019; Ouyang, 2014; Righi et al., 2015). Technical analysis often includes modelling and simulation techniques, at both network and component levels, integrating well-known concepts, such as reliability, robustness, maintainability and recoverability (Lounis & McAllister, 2016). For instance, to quantify resilience, a much-used metric in this domain is the probability that full functionality is achieved before a specific time (Barker, Ramirez-Marquez, & Rocco, 2013).

The organisational and societal domains deal with the humans and resources surrounding the system itself and are more process-oriented (McManus, Seville, Vargo, & Brunsdon, 2008). Organisations that operate and manage CIs needs to understand the processes of organisational capacity and capability, training, planning, leadership, communication, and so forth. Typically, organisational resilience is measured by using index methods in a qualitative or semi-quantitative way (see e.g. Gibson & Tarrant, 2010; Kozine & Andersen, 2015; McManus, 2008; Stephenson, 2010), and there is a growing body of literature in this field, also including acknowledged standards (American National Standard (ANSI/ASIS), 2009; International Organization for Standardization (ISO), 2011; 2014a, 2014b, 2014c). Similar methods are adapted in the societal domain, referring to the abilities of civil society, social groups, and individual to cope with CI contingencies, where most of the efforts have been directed towards development of societal/community resilience indicators (see e.g. Chang & Shinozuka, 2004; Cutter et al., 2008; Flint & Luloff, 2007; Petersen, Fallou, Reilly, & Serafinelli, 2017; Rosenqvist, Reitan, Petersen, & Lange, 2018; Sherrieb, Norris, & Galea, 2010).

As seen, CIR is a multifaceted concept, consisting of several domains. These domains inescapably influence and overlap one another. Analytically, it is justifiable to separate these domains, but, to see the bigger picture, considering CIs as socio-technical systems, the domains need to be seen in conjunction with each other. Despite the high number of promising assessment approaches, there seems to be a lack of a unified approach linking these domains together in the CIR context at a higher level, similar to what has been done in traditional risk management (e.g. ISO, 2018, 2019). Furthermore, a central part of resilience assessment is

underdeveloped, namely evaluation of the results. Evaluation should provide for what comes after an assessment, to propose the most effective measures to enhance the resilience level.

1.2 Problem definition

Based on the presented topical background, I put forward three main research problems at an overarching level that I wish to address and provide answers to in this thesis. I argue that these three problems stand out as the most important to solve in order to move CIR forward, both as a scientific discipline and at the operational level.

First, in order to utilise the CIR concept properly, I contend that the purpose and objective of CIR needs to be clearly defined. There is a common understanding of what a CI is and its importance for society. Resilience, on the other hand, is a vaguer and ambiguous concept and has been subject to a vibrant scholarly discussion in the field of safety, security and risk studies. Voices in the debate argue that it is not clear what resilience adds, compared to existing concepts such as risk, reliability and vulnerability – what do we want to achieve by introducing and operationalising CIR, and why is it better than protection?

Second, based on the objective and purpose of introducing and implementing CIR, in what ways can it be measured and assessed properly? Dependent on how CIR is defined, there should be sophisticated metrics and methods in place to measure and analyse how resilient CIs are. Furthermore, such methods should have the ability to evaluate whether the analysed resilience level is satisfactory, which again can be used as input for resilience enhancement. In the research community, numerous definitions of resilience have been proposed over the past two decades or so. Consequently, a high number of different methods to measure and analyse resilience has been developed, from more practical methods to theoretical methods. However, a common understanding of the key components that such assessments should contain seems to be missing. Moreover, the latter part of a CIR assessment, namely, how to evaluate the analysis results, as my literature review shows, is heavily underdeveloped. As CIs provide vital services to the end-user, it is essential to evaluate and compare the performance level against the end-user's expectations and tolerance levels.

Third, as an extension to the previous challenge, it is crucial that the results from a CIR assessment are utilised in an operational environment. In short, it is not enough to assess the resilience level, the CIR assessment should be part of a continuous process, whose aim is to monitor and enhance the resilience level. My claim, therefore, is that there is a need for clear guidelines and methodologies on how to operationalise and manage CIR. Such guidelines, frameworks and methodologies should be suitable for use at a system level and also at a system-of-system level, avoiding loss of generality. In addition, by integrating the organisational, technological and societal domains, they should take into account not only the risk level the CI is exposed to but also the tolerance levels of the society and the operator.

1.3 Research questions

To address and provide answers and solutions to these three problems, I propose three research questions. The research questions are directly linked to the three problems.

Research question 1 Why is CIR needed and what is CIR achieving?

Research question 2 How can CIR be measured and assessed?

Research question 3 How can CIR be operationalised and managed?

1.4 Research objectives and tasks

The overall aim of this thesis is to improve our understanding of CIR and gain knowledge on how to assess and manage CIR, at both a methodological and a theoretical level. More specifically, based on the proposed research questions, to reach this goal, as presented in Table 1, I put forward the following three objectives and associated tasks:

Table 1. Research objectives and associated research tasks

Research objectives	Research tasks
1. Explore why CIR is needed and improve the understanding of the application and interaction of different resilience concepts.	A. From a theoretical and practical perspective, review existing literature and practices, and compare it to the view of CI operators.
2. Propose and develop suitable CIR assessment techniques and methods.	A. Critical review of promising resilience metrics and assessment methodologies. B. Demonstration and evaluation of the proposed resilience assessment methods and techniques in a real-life environment.
3. Develop an overall CIR management framework that is compatible existing risk management practices and the variety of CIR assessment method and techniques.	A. Mapping CIR against definitions and concepts already used in risk management. B. Implement the framework in real-life environment by using the developed CIR assessment techniques and methods. C. Evaluate the performance of the framework with respect to a set of success factors, receiving feedback from CI operators and practitioners in the field.

1.5 Scope and limitations

I have conducted a large part of this study in association with the EU project IMPROVER - 'Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure' (2015-2018), funded from the Horizon 2020 Research and Innovation Programme under grant agreement no. 653390. Four of the papers (II, III, IV, and V) are a direct by-product of the project, while the other three papers (I, VI, and VII) are indirectly connected to the project. All seven papers address the three research questions, but to different degrees. I am co-author of two of the papers (II and IV). I clearly indicate my contribution in the summary of the papers.

In association with the IMPROVER project, the developed assessment techniques and CIR management framework have been demonstrated, tested and implemented and evaluated in a real-life environment, using so-called living labs. The main goal of this was to evaluate the performance of the developed techniques and the proposed framework, focusing on factors such as usability, measurability and tailorability. This process is clearly described in Chapter 3 – Research methodology.

As this study was executed in conjunction with an EU project, the scope is bound to the European cross-border level of CIs. However, I show examples from Norway, and one case study is limited to the national level (Paper VI).

This thesis will focus on the technological (also referred to as technical and engineering) and organisational domain of CIR but will also discuss the implications for the societal and community domains. It has not been in the scope of this study to address CI interdependencies explicitly, but I discuss some important aspects, and some of the assessment techniques encounter interdependencies indirectly. Although I discuss the results from the CIR assessments, the focus in the thesis is on *how* and *why* this should be done.

1.6 Structure of thesis

The thesis is divided into two parts. Part I provides a summary of the thesis, divided into six chapters. I start by outlining the conceptual background in Chapter 2, firstly by discussing the resilience concept in general, and, secondly, by linking resilience and CI together. This is followed by a description of the research methodology in Chapter 3, outlining how this study is conducted. In Chapter 4, I present extended summaries of all the seven appended papers, also describing shortly how each individual paper contributes to the research questions. In Chapter 5, I present and discuss the main findings in accordance with the research questions and research objectives. Finally, in Chapter 6, I provide research conclusions and propose future research initiatives.

Part II consists of all the seven papers in full length.

Part I

Chapter 1 Introduction

Chapter 2 Conceptual background

Chapter 3 Research methodology

Chapter 4 Summary of papers

Chapter 5 Results and discussions

Chapter 6 Conclusions

Part II

Papers I-VII appended.

2 Conceptual background

In this chapter, I present the conceptual background, firstly by discussing the resilience concept in general, and, secondly, by linking resilience and CI together, providing conceptual descriptions, definitions and terminology.

2.1 Resilience as a concept

Resilience has become a very popular concept in many fields, such as ecology (e.g. Walker, 1995), psychology (e.g. Fletcher & Sarkar, 2013), economic (e.g. Rose, 2004), and safety and security (e.g. Bergström et al., 2015; Hosseini et al., 2016). Figure 3, simply showing the results from a topical Web of Science search (November 2019) using the term 'resilience', illustrates the exponential growth of the overall resilience literature, especially during the period of my PhD project (2015-2019). Dependent on who you ask, you will get a wide range of descriptions of what resilience actually is. Across various fields, researchers, practitioners and policymakers interpret the meaning of the concept differently. In other words, the concept lacks a common theoretical and empirical understanding. A common debate is whether resilience is an outcome or a process (Folke, 2006; Manyena et al., 2011) and who invented and 'owns' the concept (see e.g. Alexander, 2013).

The varying descriptions and definitions of resilience, including the many attributes it contains, can at times contradict each other. This has led to some confusion and some academic voices claim that this has hindered the evolution and application of the concept (see e.g. Aven, 2019). On the other hand, others consider the conceptual vagueness an asset, bringing to the table innovation and creativity that leads to problem solving rather than puzzle solving (see e.g. Strunz, 2012).

To understand resilience, I believe it is necessary to analyse the concept in a multidisciplinary context. Furthermore, to fully utilise the resilience concept, I see the importance of taking into account the contributions from various disciplines, to understand and develop the concept into something fruitful, without defending any approach. Hence, this section will present a synthesis of literature and applications from various research fields and disciplines that are relevant in a CI context.

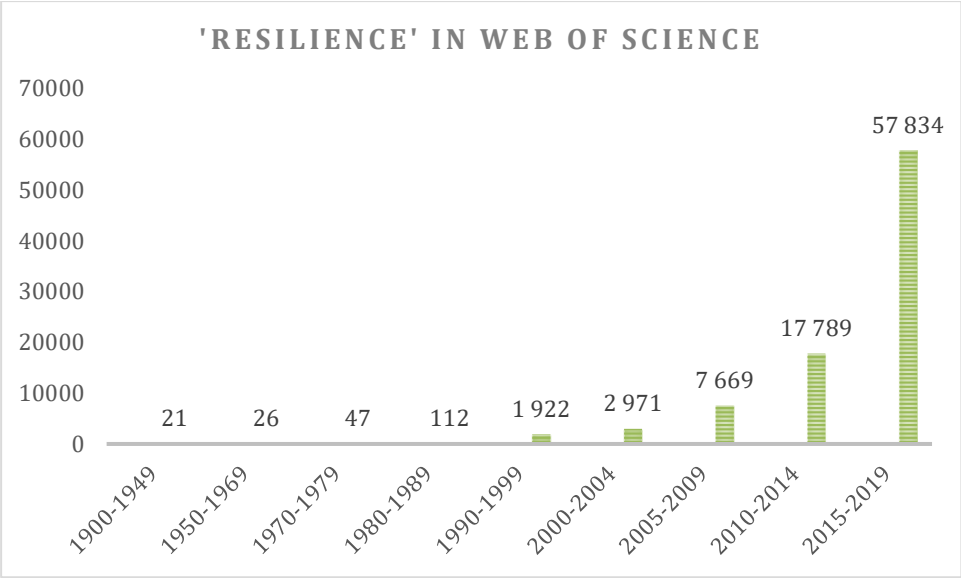

Figure 3. Web of Science topic search for the term 'resilience'

2.1.1 Origin of the concept

The word 'resilience' stems from the Latin word, 'resiliere', which means to bounce or spring back (Manyena et al., 2011). The concept was first introduced in the textile and metal industries to express the elasticity of materials. William J.M. Rankine (1829-1872) employed the concept to describe the strength and ductility of steel beams, which could be linked to some of the modern definitions of the concept, referring to an entity or system's ability to return to a normal state or functioning shortly after some disturbance (Alexander, 2013). In an academic context, the disciplines of psychology and psychiatry were the first to introduce the concept in the 1950s, investigating how the social environment might influence the development of adults and children (Waller, 2001). In ecosystem theory, Holling (1973) was one of the first to introduce the concept. Here, he describes resilience as "a measure of the persistence of systems and of their ability to absorb change and disturbances and still maintain the same relationship" (p. 14). In the same field, Pimm (1984) proposed defining resilience as "how fast the variables return towards their equilibrium following a perturbation" (p. 322). This clearly illustrates the different interpretations of the term that even exist within the same academic field.

From the 2000s, the resilience concept started to emerge in organisational and management studies (e.g.McManus, 2008; McManus et al., 2008; Riolli & Savicki, 2003; Vickers & Kouzmin, 2001), disaster risk reduction (e.g. Benson, Twigg, & Rossetto, 2007; Sapirstein, 2006; Twigg, 2007), sustainability science (e.g. Adger, 2003; Fiksel, 2006; Leach, 2008), climate change adaption (e.g. Berkes & Jolly, 2002; Hughes et al., 2003; Thomalla, Downing, Spanger - Siegfried, Han, & Rockström, 2006), and safety and security science (e.g. Bruneau et al., 2003; Hollnagel, Woods, & Leveson, 2006).

In general, based on the evolution of the concept in literature, resilience has been defined in two broad ways: as a preferred outcome or as a process oriented towards a desired outcome, bounce-back vs adaptation (Giroux & Prior, 2012; IMPROVER Project, 2016b). On one hand, resilience can be an entity's ability to return quickly after a disruption to its predefined state. On the other hand, resilience can be a process of adaption and change, suggesting that the

system's properties can change in response to the disturbance (Giroux & Prior, 2012; Manyena et al., 2011). In the following section, based on a synthesis of the existing academic literature, I will present and discuss the most important domains of resilience

2.1.2 Engineering resilience

In engineering science, resilience was introduced in the 17th century in mechanics, describing the properties of materials. Recently, other branches of engineering have adopted some of the same principles (see e.g. Righi et al., 2015). In the early 2000s, Hollnagel et al. (2006) proposed a concept called 'resilience engineering' as a method for dealing with safety and security in socio-technical systems. As stated by Nemeth and Herrera (2015), the intention is to "enable systems and organisations to continue to operate in the face of unforeseen large-scale demands, as well as to improve their everyday functioning" (p. 1). Woods (2015) highlights four concepts of resilience and presents some of the implications for the future of resilience engineering, namely "(1) resilience as rebound from trauma and return to equilibrium; (2) resilience as a synonym for robustness; (3) resilience as the opposite of brittleness, (…); (4) resilience as network architectures that can sustain the ability to adapt to future surprises as conditions evolve" (p. 5). The latter concept is related to adaptation, while the three first concepts are about reaching a desired outcome, thus showing the diversified interpretations of the concept.

In engineering, the classical way of describing resilience is the performance loss and recovery function, presented in Figure 1 and Figure 2. Typically, this function is divided into phases and temporal dimensions. For instance, Francis and Bekera (2014) focus on three resilience capacities: adaptive capacity, absorptive capacity and recoverability. As the review study of Hosseini et al. (2016) highlights, there are numerous ways to separate the temporal dimensions, for instance by anticipation, absorption, robustness, response, recovery and adaptation.

Anticipation refers to strategies aiming to predict future threats and hazards that could influence the system, including identifying inherent vulnerabilities (Panteli, Trakas, Mancarella, & Hatziargyriou, 2017). The absorptive phase starts immediately after the incident occurs, and how much the performance drops in this phase is often referred to as the level of robustness (Bruneau et al., 2003). Robustness refers to strategies related to the system's ability to resist and absorb the impact of threats and hazards, aiming to minimise the disruption (Vugrin, Warren, & Ehlen, 2011). The absorption phase is followed by the response and recovery phase, which ends when the performance is fully recovered (Pant, Barker, Ramirez-Marquez, & Rocco, 2014). Response and recovery are aimed at activities that ensure a swifter restoration of the system during the acute phase (response) of a disruption and in the aftermath (recovery) (Youn, Hu, & Wang, 2011). After the performance is recovered, the adaptation phase starts. However, ideally, adaptation would be active throughout the entire lifetime of a system. Adaptation comprises activities related to the design, redesign and implementation of measures to counteract past and future threats and hazards (Francis & Bekera, 2014). It is of course difficult to differentiate this phase from the anticipation phase, but here I consider the adaptation phase to be the time directly following the ended recovery phase, when new norms are adopted.

2.1.3 Disaster and community resilience

In disaster and crisis management, resilience is seen as the ultimate goal for reducing disaster risks (Djalante, Holley, & Thomalla, 2011). Resilience is understood as the capacity of a community, system or society potentially exposed to hazards to resist, absorb, accommodate and recover from disaster in a timely and efficient manner (UNISDR, 2009). A common way of describing resilience analytically in this context is the crisis management cycle (see e.g. Aligne & Mattioli, 2011; Pursiainen, 2017). In the same manner as the performance loss function, the crisis management cycle is divided into pre-, during and post-crisis phases, describing a continuous process. Pursiainen (2017), for instance, distinguishes between six phases: risk assessment, prevention, preparedness, response, recovery, and learning, illustrated in Figure 4. This approach is more oriented towards processes compared to engineering resilience, and it is worth noting that risk assessment is considered the first stage in the cycle.

Figure 4. The crisis management cycle (Pursiainen, 2017)

Disaster resilience also encompasses the ability of communities to cope with extraordinary situations, often referred to as community resilience. The ultimate goal is to build disaster-resilient communities, increasing their ability to withstand adversity and to recover quickly (Cutter et al., 2008). Similar to other domains of resilience, community resilience consists of different characteristics and temporal dimensions, and there is a wide range of definitions of community resilience (Zhou, Wan, & Jia, 2010). The academic literature in general differentiates between three forms of community resilience: resistance, recovery and adaptation (Boon, Cottrell, King, Stevenson, & Millar, 2012). Resistance focuses on the ability to absorb perturbations (Geis, 2000), recovery refers to communities' ability to quickly recover from external stress (Aldrich & Meyer, 2015; Paton & Johnston, 2001), while adaptation focuses on communities' capacity to self-organise to maintain functionality in the

face of change or in response to perturbations (Boon et al., 2012; Cutter et al., 2008; Maclean, Cuthill, & Ross, 2014). For instance, Magis (2010) defines community resilience as "the existence, development, and engagement of community resources by community members to thrive in an environment characterized by change, uncertainty, unpredictability, and surprise" (p. 401), indicating that community resilience is closely linked to the surrounding environment.

2.1.4 Organisational resilience

Organisational resilience has been subject to growing interest from practitioners and academics since the early 2000s. Already, in 2001, Rerup asked how an organisation remains resilient while experiencing an unexpected situation, and directed the focus towards two important attributes: anticipation and improvisation. Jordan and Alcantara (2014) claim the financial crisis of 2007-2008 induced the largest growth of organisational resilience as a concept, acknowledging the failure of conventional risk management. Not surprisingly, organisational resilience lacks a common understanding, and the term is used inconsistently (see e.g. Braes & Brooks, 2010; Burnard & Bhamra, 2011; De Bruijne, Boin, & Van Eeten, 2010; Robert & Hémond, 2012). Many definitions aim to explain organisational resilience by concentrating on different equilibrium states, operational capability and capacities, flexibility and strategic implications (see e.g. Allen, Datta, & Christopher, 2006; Crichton, Ramsay, & Kelly, 2009; Deverell & Olsson, 2010; Smith & Fischbacher, 2009). While the definitions of organisational resilience are diverging, the overall objective seems to be quite clear: to survive a certain disturbance or shock. In order to achieve that, organisations need to be adaptive, proactive and reactive, to deal with risks and threats (Braes & Brooks, 2010). Vogus and Sutcliffe (2007, p. 3481) put it quite nicely, defining organisational resilience as "the maintenance of positive adjustment under challenging conditions such that the organisation emerges from those conditions strengthened and more resourceful".

2.1.5 Economic resilience

Economic resilience, as stated by Rose and Liao (2005), refers to "the inherent ability and adaptive response that enables firms and regions to avoid maximum potential losses" (p. 76). In the economic domain, literature brings up some interesting and innovating perspectives. For instance, Simmie and Martin (2010), when discussing the economic resilience of regions, oppose the equilibrist view on resilience, arguing that "instead we should seek an understanding of the concept from an evolutionary perspective" (p. 27). Put into the performance loss function, this adds a new dimension to resilience. They claim that systems should thrive to not only bounce back but also become better than the previous "100 %". Moreover, Rose and Krausmann (2013) see some clear overlaps between community resilience and economic resilience, especially on the macroeconomic level, where the producer and consumer behaviour is a key component of group interactions. They further go on to present two types of economic resilience, static and dynamic resilience. Static economic resilience is the ability to maintain function when shocked, while dynamic economic resilience is the hastening of the speed of recovery from a shock.

2.1.6 Discussion

This clearly illustrates the different interpretations of resilience and, at the same time highlights some of the similarities and overlapping features between resilience domains. The

engineering disciplines tend to focus on systems behaviour near a stable equilibrium and, in most cases, on how fast a system returns to steady state following a disturbance. Folke (2006) sees this in contrast to what he refers to as ecological and socio-ecological concepts, as described in Table 2. The ecological and socio-ecological resilience concepts have many commonalities with organisational, disaster, and community resilience, focusing on the adaptive capacities and maintaining functionality when experiencing stress.

While Folke (2006) and Manyena et al. (2011) see resilience as either a process or an outcome (bounce back vs adaption), Handmer and Dovers (1996) introduce a three-class typology of resilience. In short, type 1 is resistance and maintenance, type 2 is change at the margins, and type 3 is openness and adaptability. Moreover, Dovers and Handmer (1992) differentiate between reactive and proactive resilience. Reactive resilience is associated with the adaptive capacity, while proactive resilience relates to humans' capacity to learn and anticipate.

Table 2. Three resilience concepts (Folke, 2006)

Resilience concepts	Characteristics	Focus on	Context
Engineering resilience	Return time, efficiency	Recovery, constancy, robustness	Vicinity of a stable equilibrium
Ecological resilience	Buffer capacity, withstand, maintain functions	Persistence, robustness	Multiple equilibria, stability landscapes
Social-ecological resilience	Interplay disturbance and reorganisation, sustaining and developing	Adaptive capacity, transformability, learning innovation	Integrated system feedback, cross-scale dynamic interactions

The discussion on the finer points of resilience is indeed interesting. Nevertheless, I think it is important to acknowledge that there is no 'one size fits all solution' in most contexts, especially when it comes to CIs and its multidimensional environment. As my study will show, whether resilience is to bounce back from disturbance or to develop resilience in an adaptive manner will strongly depend on the entity or system, discipline and operationalised context.

2.2 Critical Infrastructure Resilience

So far, I have presented and briefly discussed the resilience concept without framing it in a specific context. Here, I add CI and resilience together and present the central concepts, definitions and terminology.

2.2.1 Defining CIR

In 2005, as first step toward the 2008 European Critical Infrastructure Protection Directive, the European Commission published a green paper on a European programme for critical infrastructure protection (European Commission, 2005). In the paper, the following is stated:

> *Critical infrastructure (CI) can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. To save the lives and property of people at risk in the EU from terrorism, natural disasters and accidents, any disruptions or*

> *manipulations of CI should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States (MS), their citizens and the European Union.* (p. 2)

Although the focus of the paper is protection, this statement illustrates the concept of resilience somehow indirectly starting to make its way into policies, acknowledging that CI disruptions will occur and should be "to the extent possible" avoided. The same paper provides an indicative list of CI sectors, shown in Table 3. The list consists of 11 sectors, with 38 associated products or services. Later, in the European Directive from 2008 (The Council of the European Union, 2008), a CI is defined as follows:

> *An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.* (p. 3)

When comparing this definition with the list of CIs in Table 3, the CI concept is quite intuitive and understandable. In short, it means every infrastructure that provide a service or a product the society needs to function.

In Norway, consistent with the EU policies, the CI concept was introduced in a National Public Inquiry in 2006. Here, CI is defined as (translated) "(…)the facilities and systems that are absolutely necessary to maintain the critical functions of society which in turn covers the basic needs of the society and the population's perception of security and safety" (National Public Inquiry (NOU), 2006, p. 32). The definition covers many of the same aspects as those in the European Council definition. In addition, the population's perception of safety and security is mentioned here. Lately, Norway has slightly moved away from using the CI concept, and rather uses the term 'vital function in society'. However, as the definition emphasises, these functions are dependent on facilities and systems, namely CIs. In 2016, the Norwegian Directorate of Civil Protection (DSB) published a report (English version published in 2017) with an overview of these vital (societal) functions, as shown in Table 4. The functions are divided into three main categories: governability and sovereignty, security of the population, and societal functionality. The 14 critical societal functions are further divided into several so-called capabilities. This is slightly different from the European Commission's indicative list, but, as with the CI definition, it is evident that it covers many of the same aspects.

Table 3. Indicative List of Critical Infrastructure Sectors (European Commission, 2005)

Sector		Product or service
I	Energy	1. Oil and gas production, refining, treatment and storage, including pipelines 2. Electricity generation 3. Transmission of electricity, gas and oil 4. Distribution of electricity, gas and oil
II	Information, Communication Technologies (ICT)	5. Information system and network protection 6. Instrumentation automation and control systems 7. Internet 8. Provision of fixed telecommunications 9. Provision of mobile telecommunications 10. Radio communication and navigation 11. Satellite communication 12. Broadcasting
III	Water	13. Provision of drinking water 14. Control of water quality 15. Stemming and control of water quantity
IV	Food	16. Provision of food and safeguarding food safety and security
V	Health	17. Medical and hospital care 18. Medicines, serums, vaccines and pharmaceuticals 19. Bio-laboratories and bio-agents
VI	Financial	20. Payment services/payment structures (private) 21. Government financial assignment
VII	Public & Legal Order and Safety	22. Maintaining public & legal order, safety and security 23. Administration of justice and detention
VIII	Civil administration	24. Government functions 25. Armed forces 26. Civil administration services 27. Emergency services 28. Postal and courier services
IX	Transport	29. Road transport 30. Rail transport 31. Air traffic 32. Inland waterways transport 33. Ocean and short-sea shipping
X	Chemical and nuclear industry	34. Production and storage/processing of chemical and nuclear substances 35. Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36. Space 37. Research

Table 4. Vital functions in society, Norway (DSB, 2017)

Categories		Vital functions
I	Governability and sovereignty	1. Governance and crisis management 2. Defence
II	Security of the population	3. Law and order 4. Health and care 5. Emergency services 6. ICT security 7. Nature and the environment
III	Societal functionality	8. Security of supply 9. Water and sanitation 10. Financial services 11. Power supply 12. Electronic communication network and services 13. Transport 14. Satellite-based services

Now, having a clear understanding of the CI concept, how should CIR be defined? With the definition of resilience being contested, that is a more troublesome exercise. Defining, understanding and analysing resilience in this context is a difficult task, considering all the different stakeholders (Kahan, Allen, & George, 2009). In the US, the National Infrastructure Advisory Council (NIAC) defines infrastructure resilience as follows:

> *The ability to reduce the magnitude and/or domain of a disruptive event. The effectiveness of a resilience infrastructure or enterprise depends on its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.* (NIAC, 2009, p. 8)

This definition resembles many of the same abilities provided in the United Nations Office for Disaster Risk Reduction (UNISDR) (n.d.) definition of resilience, which was adopted by the IMPROVER project. In this thesis, I define CIR according to the IMPROVER definition (Petersen, Lange, & Theocharidou, 2020), as follows:

> **Critical Infrastructure Resilience (CIR**) is the ability of a CI system exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, for the preservation and restoration of essential societal services. (p. 3)

This is a broad CIR definition, covering all the temporal dimensions and aspects of resilience. The definitions also acknowledge that resilience can be both a preferred outcome and a process towards a desired outcome.

2.2.2 CIR domains

While the CIR definition above works well as a baseline, the CIR concept remains multifaceted. Hence, we may differentiate between several CIR domains in literature. By 'domains' I mean

separate but overlapping areas, of CIR. For instance, Labaka, Hernantes , and Sarriegi (2015) state that, in the context of infrastructure, literature characterises four different domains of resilience, namely technical, organisational, economic and social resilience, whereas Akter, Nasiruzzaman, Mahmud , and Pota (2014) highlight the three former domains. Similarly, I wish to highlight three interacting CIR domains: technological, organisational, and societal. In this thesis, I consider economic resilience as an inherent part of the three main CIR domains.

The *technological* domain, or often referred to as the engineering or technical resilience domain, deals with the physical properties of the infrastructure systems (Lange et al., 2017). Considering the performance loss function presented earlier, technical resilience focuses on the ability to reduce loss of function in an over-stress situation, by having robust, redundant, flexible and repairable systems (Francis & Bekera, 2014; Labaka et al., 2015; Youn et al., 2011). This also includes the ability of systems to fail in a safe way and, in many cases, where applicable, one may adapt the idea of 'rebuild it better' or upgradeability, to enhance the performance level of the infrastructure to a higher level than before the incident (IMPROVER Project, 2017).

Organisational resilience includes all the actors that manage the infrastructure systems. Some of the key processes here include building organisational capacity and capability, planning, leadership, training and exercises, communication, information processing and management, and so forth (Boin & McConnell, 2007). The ultimate goal of organisational resilience is to improve the organisational performance when facing abnormal situations and to incorporate a proactive and problem-solving mentality within the organisation (Burnard & Bhamra, 2011). This could be a quite complex task since organisations must consider many factors, such as strong and flexible leadership, an awareness and understanding of their operating environment, their ability to adapt in response to rapid change and so on (Lee, Vargo, & Seville, 2013).

CI systems deliver essential services to the end-users, namely the society. As an infrastructure operator, one would like to know the needs and the tolerances of the community, i.e. the *societal* resilience level (Petersen, Lundin, et al., 2020; Petersen, Lundin, Sjöström, Lange, & Teixeira, 2018; Rosenqvist et al., 2018) . Having this information at hand can help CI operators to set their minimum service levels and to make the right prioritisations, often required by the regulating authority, in order to minimise the social consequences of an interruption. Moreover, operators should raise public awareness through effective communication, illustrating the link between societal, technical, and organisational resilience. This domain is closely linked to the community or end-user, whereas organisational and technological resilience are strongly related to the infrastructure systems themselves (IMPROVER Project, 2016a). Figure 5 illustrates the overlapping and interacting CIR domains (organisational, technological and societal).

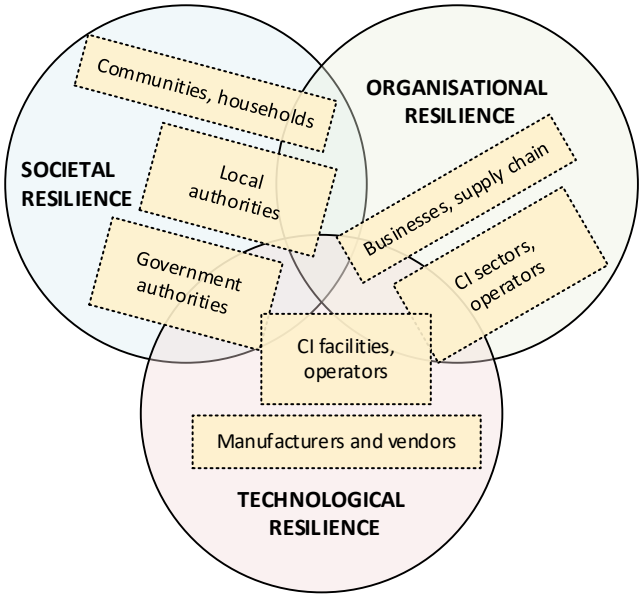

Figure 5. CIR domains. Adapted from IMPROVER Project (2016c)

2.2.3 CIR assessment

If the intention is to enable CI systems to resist, absorb, accommodate and recover from unwanted events, in practice this means findings ways to assess the existing resilience level, in order to enhance it. In analogy with the existing standards for risk management, such as ISO 31000 (ISO, 2018, 2019), a resilience assessment is characterised by two main components: resilience analysis and resilience evaluation (Lange et al., 2017), as shown in Figure 6. Resilience analysis is the process of comprehending and determining the level of resilience, while resilience evaluation in the process of comparing the analysis results against some predefined criteria, to decide whether the level of resilience is acceptable or not. In this study, I will put forward evidence to show that the latter part is underdeveloped.

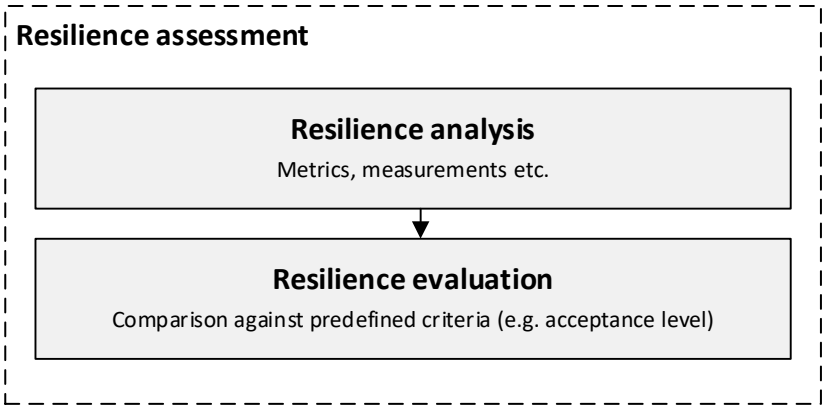

Figure 6. Resilience assessment components

Depending on how CIR is defined, and the domain(s) of interest, there are numerous approaches for assessing resilience. In this thesis, as presented in the scoping study in Paper VII, I differentiate between four overarching resilience assessment approaches, as presented in Table 5.

Table 5. CIR assessment approaches and methods

Approach	Example of methods
Modelling & Simulation	Network theory, engineering methods
Empirical	Statistical methods
Index	Aggregation of underlying data, indicator-based
Expert	Surveys, interviews

Empirical approaches typically use statistical methods to analyse historical data, constructing recovery and restoration curves. Modelling & Simulation focus on system and component level, i.e. by using engineering methods and network theory. Index approaches typically aggregates underlying data using indicators in a semi-quantitative manner, while Expert approaches often analyse qualitative data using methods such surveys and interviews.

Associated with these four approaches, I refer to assessment methods in general. When talking about one specific resilience assessment methodology, I also use the term 'resilience assessment technique'. A resilience assessment methodology can consist of several methods.

Independent of the chosen approach(es), the first step is to define a proper way to measure resilience. Since the performance loss function was introduced by Bruneau et al. (2003), a wide range of metrics has been proposed to measure CI performance over time, such as functionality (e.g. Espinoza, Panteli, Mancarella, & Rudnick, 2016; Ouyang & Wang, 2015; Yang, Ng, Zhou, Xu, & Li, 2019) and service level (e.g. Chopra, Dillon, Bilec, & Khanna, 2016; Kameshwar et al., 2019; Verma, Araújo, & Herrmann, 2014). As my scoping study shows, this type of measurement is more dominant in technical analysis, using modelling & simulation and empirical data. Empirical data is typically utilised in statistical models and regression analysis, often focusing on the recovery process. A way of measuring resilience here is in terms of recovery rate or recovery time, often referred to in conventional reliability engineering as recoverability or maintainability (see e.g. Barabadi & Ayele, 2018; Barabadi, Barabady, & Markeset, 2011; Naseri, 2017; Youn et al., 2011).

In the organisational domain, index and expert methods are prevalent, often combining qualitative and quantitative data. Cutter et al. (2008) suggest measuring organisational resilience with indicators related to hazard reduction and mitigation, emergency services, zoning and building standards, emergency response plans, continuity of operations, and so forth. Based on semi-structured interview with experts, McManus (2008) proposes fifteen organisational resilience indicators, across three dimensions (situational awareness, management of keystone vulnerabilities, and adaptive capacity). Stephenson (2010) introduced the organisational resilience measurement tool, composed of 13 indicators related to adaptive capacity and planning. In this field, there are also several international standards aiming to measure and improve organisational resilience, such as ASIS SPC.1-2009 (ANSI/ASIS, 2009) , ISO 28002:2011 (ISO, 2011), BS 65000:2014 (British Standard (BS), 2014) , and ISO/DIS 22316 (ISO, 2017).

The societal domain adopts similar methods. For instance, Rosenqvist et al. (2018) propose measuring societal resilience with specific indicators categorised across six capacities: physical, social, human, natural, economic and institutional.

Based on the resilience assessment results, one should propose options to improve and enhance the resilience level, similar to the risk treatment phase in traditional risk management. Ideally, a CIR assessment should analyse the effect of enhancement options.

As *how* to assess and operationalise CIR is a central research question in this thesis, I will thoroughly present and discuss this in greater detail in Chapter 3 – 5.

3 Research methodology

In this chapter, I present the research methodology in the project. In short, this means how to get an answer to the proposed research questions. First, I present the overall research strategy and design. Second, I give an overview of the data collection and extraction process, now going into greater detail on each of the specific papers. Third, I present how I have analysed the collected data and extracted data. Last, I discuss the research quality of this study.

3.1 Research strategy and design

As seen, CIR is a multifaceted subject, including many disciplines and academic fields. In such an environment, design science is considered a suitable research methodology, where the goal is to operationalise research by designing and creating artefacts and finding solutions to given problems (Dresch, Lacerda, & Antunes, 2015). Dresch et al. (2015) present a strategy for carrying out scientific research in this context, divided into seven steps, illustrated in Figure 7. A similar approach has been adopted for this study.

Figure 7. Design science research strategy. Adopted from Dresch et al. (2015)

In the introduction, I clearly defined the research problem and proposed a set of research questions with associated objectives, hence presenting the reason behind the study and the study's goals. In accordance with Figure 7 , I here present the overall research strategy for this study.

A scientific method refers to "a body of techniques for investigating phenomena, acquiring new knowledge, or correcting and integrating previous knowledge" (Seel, 2011, p. 2974). A scientific method can typically be divided into three branches: induction, deduction, and abduction (e.g. Dresch et al., 2015; Flach & Kakas, 2000; Kudo, Murai, & Akama, 2009; Staat, 1993; Thornhill, Saunders, & Lewis, 2009; Yu, 1994). Induction as a scientific method looks for patterns in gathered data, as the basis for developing theories (Flach & Kakas, 2000). Deduction is the opposite, starting with theorising the problem and then analysing data to see whether the hypothesis is supported or not (Kudo et al., 2009). The last approach, abduction, is applied to

find the best explanations for observed facts (Flach & Kakas, 2000; Seel, 2011). For this research study, I have used these approaches for reasoning, in conjunction with each other.

In the CIR environment, design research can be used to modify existing solutions that can be used in real-life applications. Hevner and Chatterjee (2010) state that design science research methodology (DSRM) incorporates principles, practices, and process models, which are adequate to conduct design science research in applied research disciplines, whose cultures value incrementally effective solutions. The design science paradigm seeks to create and evaluate "what is effective" in the problem space (Hevner, March, Park, & Ram, 2004). Peffers, Tuunanen, Rothenberger , and Chatterjee (2007) outline the DSRM as an iterative process, describing each sequential step, shown in Figure 8. In this regard, the present research study aims to provide solutions on *how* to operationalise CIR and modify existing approaches and methodologies.

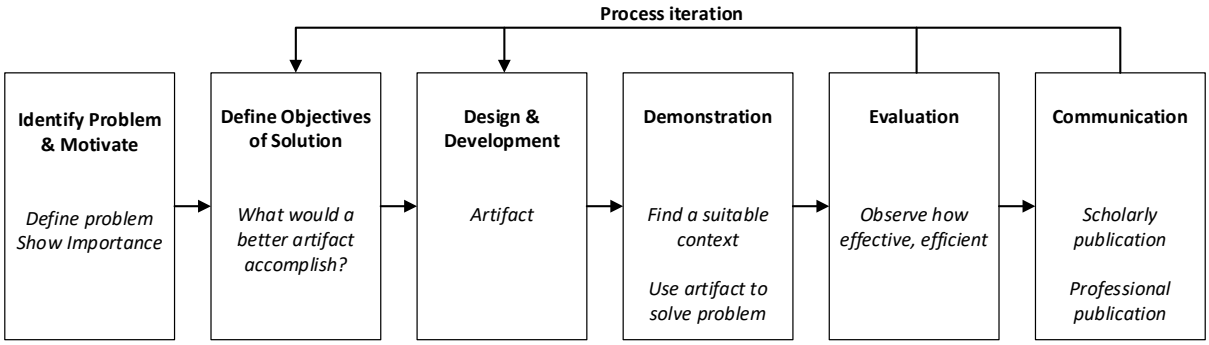

Figure 8. Design Science Research Methodology (DSRM) (Peffers et al., 2007)

As this study has been connected to the IMPROVER project, it is natural that it has a similar design. The IMPROVER project was divided into seven interacting and overlapping work packages. I here differentiate between four sequential steps, where steps 2 and 3 are considered an iterative process similar to the DSRM process outlined in Figure 8. Figure 9 describes the overall process for this study, connecting each of the seven papers to the process. These steps are linked to the research tasks proposed in Section 1.4. For each of these steps I have used suitable research methods, work methods, and techniques for data collection and analysis.

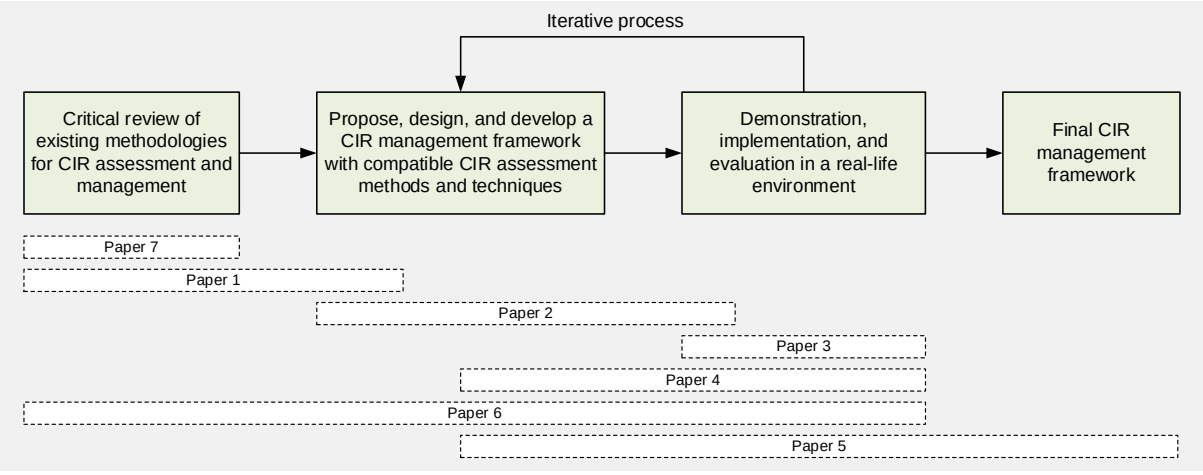

Figure 9. Research process and strategy for this study

3.2 Research methods

In design science, there are various suitable research methods, such as surveys, action research, case studies, fields studies, modelling and simulation, and so forth (Dresch et al., 2015). Using recognised research methods helps produce transparent and reliable results. In this study, I have combined several data sources, methodological approaches, theoretical perspectives, and analytical methods, often referred to as triangulation (Denzin, 1978; Kimchi, Polivka, & Stevenson, 1991). Using multiple methods decreases the "deficiencies and biases that stem from any single method" (Mitchell, 1986, p. 19) and creates "the potential for counterbalancing flaws or the weaknesses of one method with the strengths of another" (p. 21).

Papers II to V are direct by-products of the IMPROVER project and are thus conducted within the environment facilitated by the project. The IMPROVER project used real-life infrastructures, so-called 'living labs', to demonstrate, implement and evaluate the performance of the resilience assessment techniques and the management framework. These can be considered field and case studies. Field studies require detailed observation and evaluation, allowing the conclusion of understanding and comparison of the information generated from each site (Burgess, 1984; Denzin & Lincoln, 2011; Rossman & Rallis, 2016). A case study is defined as "a research strategy that involves the empirical investigation of a particular contemporary phenomenon within its real-life context, using multiple sources of evidence" (Thornhill et al., 2009, p. 588). In addition, these papers includes desktop demonstration, surveys, expert judgement, and focus groups as research methods. Focus groups, as a qualitative, explanatory method, aid the understanding about not only the participants' opinions but also how and why they think the way they do.

In paper I and VII, a review and scoping study (Arksey & O'Malley, 2005; Daudt, van Mossel, & Scott, 2013; Levac, Colquhoun, & O'Brien, 2010) was conducted, to identify and collect relevant studies. Paper I also proposes one resilience metric and provides a simple illustration of its application. Paper VI proposes a statistical model, to model the recovery time of disrupted CIs in the presence of unobserved and observed risk factors. The application and implications of the model are presented in a case study.

3.3 Data collection

In order to achieve the goals and the objectives of this study, various types of data and information were collected, using appropriate and suitable techniques. In this section, I present the data collection procedure, paper by paper.

In Paper I, I conducted a comprehensive literature review, to identify promising resilience assessment metrics and approaches. A similar approach was taken in Paper VII, but in a more structured and systematic way. The scope of the study was limited to scientific literature that assess resilience of real-life infrastructures, either single or independent infrastructures. A systematic search using the Scopus database was conducted with the search terms given in Table 6, limiting the search to scientific journal articles written in English. The Scopus database is one of the largest databases of peer-reviewed literature, with content from 24,600 active titles and 5,000 publishers. This resulted in an initial list of 354 potentially relevant articles. In the second stage, the abstracts and titles of the papers were subjected to a first review based on their relevance. Those paper identified as relevant were in a thirst stage

subjected to a full-text review. The fundamentals of the inclusion of articles were that they needed to express a clear connection with the concept of resilience and have a clear 'real-life' CI applied scope. The final papers for a full-review are hence in general presenting case studies of 'real-life' infrastructures by measuring, analysing or assessing resilience in some way. In the second stage, 52 articles were deemed relevant. However, in the full-text review in stage three, 15 articles were deemed not to fulfil the criteria, hence ending up with 37 included articles from the Scopus Database search. Based on references in these included articles and other complementing articles of relevance known by the authors, an additional 13 articles were also included. In total, 50 articles were included in the final review. The overall process is illustrated in Figure 10.

Table 6. Search criteria for scoping study

Search strings	
Query	TITLE-ABS-KEY
Concept	"Resilienc*"
Context	"Infrastruct*" w/0 "Critical" OR "Lifeline" OR "Societal" OR "Vital" OR "National" OR "Protection" OR "System"
Application	"Case stud*" OR "real-life" OR "empiric*" OR "appli*"
Constraint type of paper	
Query	DOCTYPE
Type	Journal paper (ar) OR Review (re)
Query	LIMIT-TO
Language	English (En)
Full search string	
Query	(TITLE-ABS-KEY ("Resilienc*" AND ("Infrastruct*" w/0 "Critical" OR "Lifeline" OR "Societal" OR "Vital" OR "National" OR "Protection" OR "System")) AND ("Case stud*" OR "real-life" OR "empiric*" OR "appli*")) AND (DOCTYPE (ar OR re)) AND (LIMIT-TO (LANGUAGE, "En")))

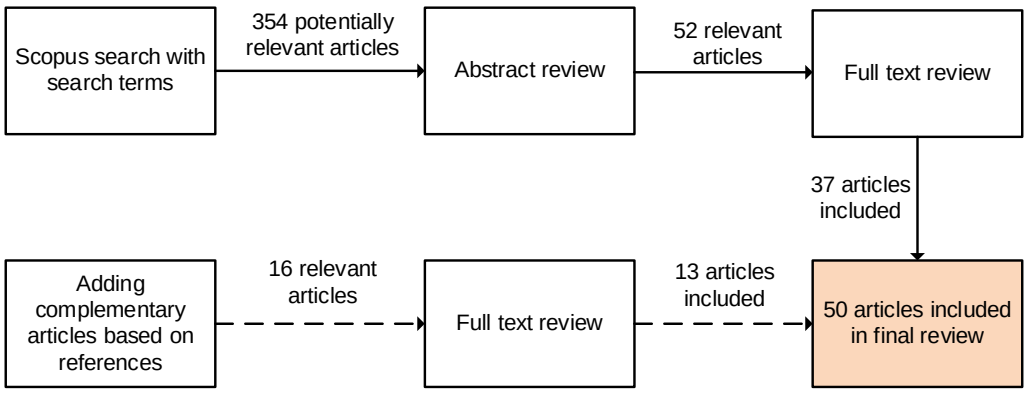

Figure 10. Scoping study procedure

Paper II draws on, combines, and develop the ideas and practices of the existing literature to develop a holistic, easy-to-use and computable methodology, to assess CIR.

Paper III collects data through a desk-top demonstration, to evaluate resilience assessment methodologies. The demonstration was done by designing case hazard scenarios for two of the living labs in the IMPROVER project: the Port of Oslo, Norway, and the Barreiro Water Distribution Network, Portugal. To test the methodologies, a set of indicators was selected relevant to the case scenarios. These indicators were then applied to the methodologies for each of the case scenarios, by using the indicators individually and in combination.

In Papers IV and V, to collect the necessary data, the proposed resilience management framework and its associated resilience assessment techniques were tested in two pilot implementations in the IMPROVER living labs. In addition, six interactive workshops were organised by the project. Participants included the project's associate partners (representatives of CI owners and operators throughout Europe), advisory board members (such as blue-light organisations and experts in resilience), CI stakeholders who are part of the EPCIP network, as well as academic and other relevant stakeholders interested in CI and resilience (Petersen, Lange, et al., 2020). A brief description of each workshop, where the data was collected, analysed and formalised into the proposed CIR management scheme, can be found in Table 7.

Paper IV is based on an initial demonstration and pilot implementation in one of the living labs, namely the potable water distribution network in Barreiro, while Paper V uses data collected from all of the workshop and pilot implementations. Focus groups, documentation, field studies and surveys were used to collect data for the critical evaluation of the performance of the resilience management framework and its associated resilience assessment techniques. A focus group, consisting of representatives from the operator at the living labs, was selected, based on their insights into current processes and methodologies for risk assessment. Throughout the IMPROVER project, close cooperation between the focus group and the project team was maintained via continuous communication and workshops. These were vital for addressing the strengths and weaknesses of the resilience management framework before the final pilot implementation. Field studies were performed to test the application of the resilience management framework in a semi-real environment. The field studies relied on an application of the proposed resilience management framework to a relevant hazard scenario. A scenario with high disaster risk was prioritised by structured expert judgement. Documentation was collected, in order to analyse vital data from the CI, for example the safety plans and technical and organisational procedures. These documents were used to assess the as-is situation of the CI. Typically, the analysis aims to visualise the current state process, to clarify how the CI process works at the time and what can be done to improve the current situation.

Different forms of surveys, aimed at the operator, project team members in IMPROVER and other stakeholders were used in advance, during and after the pilot implementations. Through the use of surveys, a broad range of data was collected, such as tolerance levels, attitudes, opinions, beliefs, values, behaviour and facts. The surveys were used as a basis both for defining performance criteria for resilience assessment and for the critical evaluation of the performance of the resilience management framework.

Table 7. Overview of IMPROVER project workshops

Date and location	Type of workshop	Topic	Participants
September 25, 2015, Copenhagen, Denmark	Associate partners Workshop I	The definition of resilience and resilience in critical infrastructure	35 participants: Critical Infrastructure operators and stakeholders, civil contingencies agencies, and academics
April 27-28, 2016, Ispra, Italy	Operators Workshop I	Organisational resilience of CI operators, resilience indicators of CI operators, and community resilience	50 participants: CI operators, representatives of governmental services, and civil protection, infrastructure protection and resilience experts
October 13, 2016, Paris, France	Associate partners Workshop II	How critical infrastructure can meet public expectations in response to a crisis	39 participants: Critical Infrastructure operators and stakeholders, civil contingencies agencies, and academics
May 11-12, 2017, Ispra, Italy	Operators Workshop II	Organisational and community resilience	54 participants: CI operators, representatives of governmental services, and civil protection, infrastructure protection and resilience experts
September 21, 2017, London, UK	Associate partners Workshop III	Usability and success criteria for the CIR management framework	35 participants: Critical Infrastructure operators and stakeholders, civil contingencies agencies, and academics
January 30-31, 2018, Lisbon, Portugal	Pilot Implementation Workshop I	Implementation, testing and evaluation of the resilience management framework in a semi-real environment (Water Distribution System)	~30 participants: CI operators, local governmental services, associated partners and researchers
May 23-24, 2018, Lisbon, Portugal	Operators Workshop III	Resilience Assessment for Critical Infrastructures: Methods and Tools (Day 1), and Resilience Enhancement for critical infrastructures: Guidelines and Standards (Day 2)	51 participants: CI operators, representatives of governmental services, and civil protection, infrastructure protection and resilience experts
May 29-30, 2018, Budapest, Hungary	Pilot Implementation Workshop II	Implementation, testing and evaluation of the resilience management framework in a semi-real environment (M1 Highway, Budapest)	~25 participants: CI operators, local governmental services, associated partners and researchers

Due to the sensitivity of the data provided by the operator, some of the demonstrations and implementations did include fictional data. However, the objective of the demonstrations and implementations was to evaluate the performance, usability and application of the resilience assessment techniques and the resilience management framework, not solely focusing on the output from the assessment. Hence, I believe the use of hypothetical values – which have also been proven to be effective in other studies (Ibbs & Nguyen, 2007; Mostafa & El-Gohary, 2014)

– to be justified. Notwithstanding the fictional data, using the well-known Technological Readiness Level (TRL) scale in the form applied by the EU, this represents TRL 7 (of 9), namely system prototype demonstration in an operational environment.

In Paper VI, data was collected and extracted from 73 interruption reports from electric power distribution companies, reported from 2013 to 2016, after four extreme weather events, namely 'Hilde'. 'Ivar', 'Tor', and 'Nina'. This data is partly sensitive, and only minor parts of the reports are publicly available. An overview of the content of the reports are given in Table 8. Through an agreement with the regulator, I was granted access to data from six extreme weather events. However, due to inconsistency in the reporting procedure, only four of the events were selected for further analysis. Moreover, the four selected weather events have quite similar characteristics, which is believed to be an advantage when comparing the recovery processes. Each grid company affected by an extreme weather event (causing power outage) is committed to deliver reports to the national regulating authority. The data used in the case study is based on such reports. From these reports, data was collected and extracted, and a set of covariates was chosen for inclusion in the analysis. Due to the quality of the reported data and the limited number of data points (n=73), a few key variables were selected for inclusion in the analysis. Many of the reports contained incomplete data and, hence, some report metrics in the reports were excluded for the analysis. The selection of variables was based on a literature review and recommendations from the regulator.

Table 8. Summary of reported data

Report metric	**Sub-categories/metric**	**Description**
County		19 Norwegian counties
Time and date		Time and date of impact
Place	City, urban and rural	Description of place (more than one is possible)
Natural conditions causing failures	Lightning, precipitation/flooding, Vegetation/trees, wind, salting, avalanche, pollution, fire, birds/animals	Qualitative description of the natural conditions that caused failures
Technical failures	Wear, mechanical failure, heat, electrical failure, fatigue, corrosion	Qualitative description of the types of technical failures
Number of persons involved in the recovery process	Internal employees, external entrepreneurs, landowners, other resources	Operators points out the number of persons involved in the recovery process, divided in four categories.
Costs	Production loss, material costs, KILE-costs, labor costs, compensation costs, other.	Operator estimate the cost out the outages caused by the storm, divided in six categories.
Damage in the grid	Transmission grid , regional grid, distribution grid	Operator states which objects in the grid that is affected, and at which voltage level.
Stations affected	Transmission grid , regional grid, distribution grid	Operator states stations that are damaged (transformation station or connecting station),
Customers without power supply	0-1 hrs., 1-6 hrs., 6-12 hrs., 12-24 hrs., 24-36 hrs., 36- 48 hrs., 2-3 days, 3-4 days, ...7-8 days.	Number of customers without power supply reported in time intervals

3.4 Data analysis

Paper II presents the Critical Infrastructure Resilience Index (CIRI). To illustrate its usability, the paper provides a simple demonstration. Paper III evaluates the performance and usability of CIRI and six other methodologies, based on a set of criteria. Table 9 presents the selection and evaluation criteria. Of the seven methodologies, based on the criteria, three methodologies were shortlisted. The evaluation based on these criteria is inspired by the work of Prat, Comyn-Wattiau , and Akoka (2015). Based on desktop demonstrations, a qualitative evaluation of the methodologies against each of the criteria in Table 9 was performed.

Table 9. Selection and evaluation criteria

No.	Weight	Criteria
1	0.17	The methodology shall have features relevant to one or more of the expected impacts of the European Commission research topic, 'Crises and disaster resilience – operationalising resilience concepts' (DRS – 07 -14)
2	0.17	The methodology shall be applicable to all types of CIs
3	0.17	The methodology shall take cascading effects into account
4	0.13	The methodology shall apply within all resilience domains, either one by one, or altogether
5	0.13	The methodology shall provide qualitative, quantitative, and semi-quantitative assessments
6	0.13	The methodology shall be user-friendly and low-cost
7	0.08	The methodology shall provide self-audit
8	0.08	The methodology shall supply already existing practice for risk and resilience management
9	0.08	The methodology shall include individual components (assessments / inventories) with different hazards, safety targets, design lifetimes, etc.
10	0.04	The methodology shall provide a sufficient balance between complexity and simplicity, as well as between specificity and generality
11	0.04	The methodology shall balance the level of resilience that CI is exposed to, with the level of resilience operators that society is willing to accept
12	0.04	The methodology shall provide relative resilience measurements, e.g. by monitoring own resilience to other CIs

The evaluation process sums up the performance of each of the methodologies in the different evaluations against the individual criteria. In this way, it is possible to determine how well each methodology fulfils the individual criteria. An overall evaluation is then carried out, by summing the ability to fulfil all of the criteria for individual methodologies. The score of the methodologies against each of the criteria is given by the following equation:

$$S_{Ci} = \sum_{\forall\, evaluations} X_{i,j}\ w_i \qquad (1)$$

where S_{Ci} is the score of how well the methodology fulfils the criteria i; $X_{i,j}$ is the assessment of how well the different methodologies fulfil the criteria *i* in the evaluation *j*. The weighting w_i represents the importance of each of the criteria in achieving the desired results within the

project. These are weighted according to simple low (0.04), medium (0.08) and high priority (0.17), according to the priority order of the criteria. The evaluation scores were only intended to give a qualitative indication of the relative performance of each of these methodologies against the different criteria.

In Paper IV, the list of criteria was extended to eighteen so-called success factors, shown in Table 10. These success factors were used for the critical performance of the proposed resilience management framework and its associated resilience assessment techniques. The success factors ensure that the framework meets stakeholders' and end-users' needs and are designed based on continuous input from the living labs during the IMPROVER project. The defined success factors of the project are primarily designed for critical evaluation of the over all resilience management frameworks, but they also implicitly set requirements regarding the relevance and quality of the tested assessment techniques. In the same manner as Paper III, the design science research methodology (Hevner et al., 2004; Prat et al., 2015) is used for the critical evaluation process, in which the success factors are evaluated based on demonstration results and applications of the resilience management framework.

Table 10. Success factors

No.	Success factors
1	The framework shall be applicable to all types of CIs
2	The framework can be applied within several resilience domains (e.g. technological, organisational, and societal), either one by one or altogether
3	The framework shall be easy to use
4	Using the framework is safe and secure
5	The framework provides efficient uptake of risk assessments
6	Effective and coherent crisis and disaster resilience management
7	Availability of tools and guidelines
8	The framework shall provide relative resilience measurements (e.g. by monitoring own resilience over time or comparing own resilience to other CIs)
9	The framework shall be low-cost
10	The framework shall take cascading effects into account
11	The framework shall provide a sufficient balance between complexity and simplicity, as well as between specificity and generality
12	The framework shall supplement already existing practice for risk or resilience management
13	The framework shall take into account the communication and interaction with the public
14	The framework shall provide self-assessment
15	The framework is arranged to be revised continuously
16	Standardisation
17	Learning capabilities
18	Willingness of utilisation

Paper V takes a similar approach when evaluating the performance of the resilience framework but also includes input from all the IMPROVER workshops (Table 7).

In Paper VI, a statistical model is proposed and applied to analyse collected recovery data of electric power distribution systems. The accelerated failure time (AFT) model is extended and applied in a case study, to analyse the recoverability of the disrupted infrastructures, in addition to analysing the impact of observed and unobserved risk factors on the recovery time. This is achieved by considering the operating conditions and other covariates, where the recovery time is selected as the random variable of interest.

In the scoping study in Paper VII, the content of the included papers was subjected to a systematic content analysis (e.g. Hsieh & Shannon, 2005; Mayring, 2004; Neuendorf, 2016). The approach employed for this was to construct a classification scheme with respect to a number of perspectives of interest. In total, the study includes 13 main categories in its analysis.

3.5 Research quality

This study is model- and process-oriented, aiming to develop reliable and valid methodologies for assessing and managing CIR. The study is mainly conceptual but tested through demonstration and implementations. No matter which type of methodology (quantitative, semi-quantitative or qualitative) one uses, one should demand some kind of reliability from a CIR assessment. The output is reliable and replicable if the assessment can be obtained irrespective of who gathers the information or designs the information-gathering (Yin, 2017). In order to ensure reliable results, the methodologies use quantitative data that is repeatable and measureable, while the qualitative data is auditable and consistent (Golafshani, 2003; Mayring, 2004). Certainly, there are some limitations in the data collection procedure, which influence the quality of the data and the analysis results. For instance, in Paper VI, the collected data are based on reports from the electricity grid operators. The structure of the reports and the way the questions are formulated leave considerable room for subjective evaluations by the operator. Moreover, as some of the raw data are qualitative and descriptive, the results will, to some extent, depend on the author's interpretation in the data extraction process. The vagueness in the data will, of course, influence the reliability of the analysis.

While the methodology might be reliable, it does not mean that it is valid (Creswell & Miller, 2000; Noble & Smith, 2015; Whittemore, Chase, & Mandle, 2001). In general, validity of research can be defined as a hierarchy of procedures to ensure that what we conclude from a research study can be stated with some confidence (Mentzer & Flint, 1997). In this context, validity is best understood to the extent that the methodology assesses the right elements of the issue one wants to assess. It is usual to differentiate between external and internal validity (e.g. McDermott, 2011; Onwuegbuzie, 2000). In this study, internal validity is ensured by demonstrating, testing and operationalising the developed resilience assessment techniques and the overall framework in case studies in a real-life environment, using so-called living labs. In relation to the IMPROVER project, a pilot implementation was carried out in a water distribution network in the municipality of Barreiro, Portugal. Using the Technological Readiness Level (TRL) scale in the form applied by the EU, this represents TRL 7 (of 9), namely system prototype demonstration in an operational environment. The case study of the Norwegian electricity grid in Paper VI can be characterised in the same manner. However,

validating the developed AFT model analytically will require many observations. One possibility could be to divide the data into two groups, and the model is then run for either of those groups, in order to estimate the model coefficients. A specification test can further be performed, to check whether or not the estimated coefficients corresponding to these two groups of data are statistically equal. However, one of the main limitations in the study in Paper VI was lack of a large database. In this regard, the results of the current study should be used with caution. By using more data in the future, the model can be run again and validated. However, the findings in the study are consistent with the evaluations performed by the regulator

External validity is ensured by providing case studies that are representative and developing an overall framework that is generic and tailorable to any CI and sector. Through several workshops throughout my project, as presented in Table 7, I received valuable feedback from academics, operators, regulators, and decision makers. At the same time, in the domain of crisis and rare events, I acknowledge that the criteria of reliability and validity can be problematic, since uncertainties are extensive (Aven, 2016; Gundel, 2005; Veenema & Woolsey, 2003). A timely question is whether a CIR assessment can be valid and reliable if omitting some crucial elements that only become evident in hindsight.

With respect to the scoping study in Paper VII, there are two main aspects that could influence the quality of the study and the conclusions drawn. First, with respect to completeness of the study, it is to some degree uncertain if all relevant studies have been identified. We tried to minimize this uncertainty by using a broad search string in one of the largest available databases for scientific publications to capture as many articles as possible. This lead to the initial identification of 354 potentially relevant articles, where 37 of these were deemed relevant for a full-text review given the aim of the study. Additional 13 articles were identified based on references in the articles or through prior knowledge by the authors. Hence, it is our belief that the scoping has a high degree of completeness and the conclusions drawn with respect to this have a high degree of validity. Second, utilizing a categorization scheme for the content analysis means that other potentially relevant aspects of the articles were not assessed. We tried to address this by letting the content of the articles iteratively influence the categorization scheme as to include as many and as correct categorizations as possible. However, fitting the content of an article into specific categories comes occasionally with a degree of subjective judgement calls. Hence, resulting in the possibility of misinterpretation of the aim or content of the articles. We tried to minimize this uncertainty by iteratively refining the categorization scheme and by also allowing for multiple instances for a specific categorization, for example allowing for categorization of multiple methods and not only the main method used.

In general, to assess reliability and validity, this study exploited the evaluation forms proposed by Hevner et al. (2004), including analytical, observational, experimental, testing, and descriptive forms.

4 Summary of papers

This chapter provides extended summaries of the seven appended papers.

4.1 Paper I

The paper focuses on resilience of Arctic infrastructures. The main objective is to develop and demonstrate a practical approach for characterising the resilience of Arctic infrastructure systems, based on expert judgement. We argue that there is a lack of clear methodologies for resilience analysis, considering the scarce amount of data and information in the Arctic context. Hence, we emphasise the need for a practical approach. The paper contributes to all research questions (RQs), albeit to different degrees.

The paper first presents a comprehensive review of resilience quantification methods, highlighting the most promising and acknowledged resilience metrics. The focus is on the engineering and technological domain, but we stress that organisational resilience certainly is part of the equation when discussing infrastructure resilience. Based on this review, we present a methodology to analyse resilience, inspired by the work of Chang, McDaniels, Fox, Dhariwal , and Longstaff (2014) and Youn et al. (2011). First, we propose a probabilistic formulation of resilience as the sum of reliability and recoverability, where recoverability is dependent on the resilience of the organisation, maintainability, and prognostic and health management (PHM) efficiency. Second, we outline a step-by-step guideline to analyse and assess resilience. Third, a simple demonstration illustrates the application of the methodology.

In the concluding remarks, we emphasise that the proposed resilience formulation captures both the effect of pre- and post-disaster activities, which we believe is a central aspect of the resilience concept. Moreover, we acknowledge that interdependencies are not directly addressed in this methodology and point out that it has not been in the scope of the paper to perform a comprehensive analysis of organisational resilience. This paper is connected to Paper VI, which address the post-event aspect of the proposed formulation, namely recoverability.

4.2 Paper II

The purpose of this paper – drawing on, combining and developing the ideas of existing literature and practices – is to develop a holistic, easy-to-use and computable methodology to assess CIR, called the Critical Infrastructure Resilience Index (CIRI). In short, how do we know whether a CI is resilient or not, and how can it be measured, assessed and enhanced? The paper contributes to RQ2 and partly to RQ 1 and RQ3.

CIRI is an index method that classifies indicators under seven crisis management cycle phases, describing the temporal dimensions of resilience, referred to as resilience phases at Level 1 (Risk assessment, Prevention, Preparedness, Warning, Response, Recovery and Learning), components and processes at Level 2 (referred to in the paper as generic indicators), generic indicators at Level 3, and finally sector-specific and actually addressed indicators at Level 4. Thus, measuring Level 4 indicators first, the measurements accumulate upwards through a scaling process producing comparable results. This is carried out using a semi-quantitative maturity scale inspired by COBIT 4.1 (Control Objectives for Information Technologies (COBIT), 2007). The output of CIRI is either an overall index, representing the accumulated resilience level with a maturity scale value or a breakdown of the maturity in the different phases.

The methodology can be tailored to the specific needs of different sectors and facilities, as well as hazard scenarios. The aim, and the innovative potential, is to be able to transfer the quantitative and semi-quantitative assessments of individual sector-specific resilience indicators into uniform metrics, based on maturity process levels.

In this paper, CIRI is demonstrated with a fictional example, for illustrative purposes, but, later, in the IMPROVER project, the technique was implemented and operationalised in a real-life environment. Hence, the paper addresses RQ2. A minor part of this operationalising process is presented in Papers IV and V. Moreover, in Paper III the CIRI technique is evaluated, together with six other resilience assessment techniques.

4.3 Paper III

The paper aims to evaluate, through demonstrations and comparison, a selection of promising resilience assessment techniques, addressing RQ2. The output from the evaluation formed the basis for the development of the CIR management framework.

Based on a set of selection criteria, seven techniques were long listed, three of which were subject to a thorough evaluation. The three techniques were the Critical Infrastructure Resilience Index (CIRI) (Bertocchi et al., 2016), Guidelines for Critical Infrastructure Resilience Evaluation (CIRE), and the Benchmark Resilience Tool (BRT) (Lee et al., 2013). A desktop demonstration was executed to collect data for the evaluation of the techniques. The demonstration was done by designing case hazard scenarios for two of the living labs in the IMPROVER project: the Port of Oslo, Norway, and the Barreiro Water Distribution Network, Portugal. To test the methodologies, a set of indicators was selected, relevant to the case scenarios. These indicators were then applied to the methodologies for each of the case scenarios, by using the indicators individually and in combination. The techniques were compared with regard to twelve desirable criteria.

The feedback from the demonstration and evaluation was mixed. All techniques had pros and cons. As there are is no strictly objective way to evaluate the techniques, much will depend on what one wants to do with a resilience assessment technique, the amount of effort and time available, and who is doing it. All the techniques end up quantifying the resilience with a final score. However, what the score actually means is dependent on the interpretation of the end-user, and there is no clear guidance on how the results should be used to enhance resilience.

In the paper, we conclude that the IMPROVER project should aim to develop a CI resilience assessment framework which is well defined but which, at the same time, also includes flexibility to account for the idiosyncrasies of the different types of CIs and their operators. Moreover, such a general framework (presented in Papers IV and V) for resilience assessment and management of CIs should remain compatible with the current guidelines for risk assessment and management of the EU Member States and should integrate the paradigm of resilience into the risk assessment and management process, in according with the risk management standard ISO 31000. In other words, the paper also contributes to RQ3.

4.4 Paper IV

This is the first paper that presents the proposed resilience management framework, here referred to as the IMPROVER Critical Infrastructure Resilience Framework (ICI-REF). To address the overall goal in the IMPROVER project – to improve European CI resilience to crisis and disaster, through the implementation of the technological, organisational, and societal resilience concept – the project developed the CIR management framework. The framework is supported by resilience assessment techniques, in the way that it loosely defined, allowing the operator to use any suitable resilience assessment technique. Thus, the paper addresses both RQ 2 and RQ 3, and also RQ 1 to a minor degree. I co-authored this paper, and my main contribution was with respect to developing the framework and demonstrating one of the resilience assessment techniques, namely CIRI (as presented in Papers II and III).

To ensure that the developed framework is fit for purpose, it was optimised in pilot implementations, by application to relevant scenarios in semi-real environments at several so-called living labs. The paper describes the pilot implementation in the Water Distribution Network in Barreiro, Portugal. The paper describes the structures and process of the framework and presents three associated resilience assessment techniques: the Critical Infrastructure Resilience Index (CIRI), the IMPROVER Technological Resilience Analysis (ITRA), and the IMPROVER Organisational Resilience Analysis (IORA).

An initial demonstration applied all three resilience assessment techniques. Evaluation from ITRA showed that the system would most probably meet the end-users' expectations for reasonable damage scenarios. The results from both ITRA and IORA show that the flat organisational structure helps with fast recovery in times of crisis. A set of indicators was tested using CIRI. The operator assigned resilience measurement scores to the indicators and rated them according to how well they were understood.

The structure and processes of resilience analysis techniques proved functional in the demonstrations. Based on the feedback from the operator, only minor modifications of the methodologies were required to optimise the relevance of the analysis results towards the main pilot implementation. This was mostly related to user-friendliness, clear and not too complex

assessments, the crucial role of resilience indicators in the monitoring of resilience activities, and needs to ensure objectivity, consistency and repeatability and create representative results. As long as the indicators are well described and leave little room for subjectivity, the high number of indicators is not a problem. The operator highlighted, among other things, the need for clear guidelines and defined measurement scales for indicators, to actually know what to measure.

The assessment results from CIRI in the pilot implementation indicated that the operator should prevent silos (i.e. to have quick and easy cooperation between management and people in the field) and have structures in place to ensure this. The implementation also shows that different resilience assessment techniques have the ability to bring up different levels of details and different perspectives. For instance, IORA identifies that the silo-preventing mechanisms already exist in the organisation, albeit as an unofficial way of working.

Adjustment from the initial demonstration made the indicators (CIRI) easier to interpret. The operator was of the opinion that the resilience framework can be valuable, both as an internal audit tool and also in everyday work, and that it was useful in promoting reflection regarding the resilience of the organisation and resilience enhancement. The ability to compare results with other operators in the sector outside Portugal would also be useful for benchmarking purposes.

The results and feedback from this pilot implementation were used to fine-tune and adjust the framework for the second pilot implementation and the critical evaluation. Paper V presents the final framework, also taking into account feedback from the second pilot implementation.

4.5 Paper V

The paper discusses CIR in terms of how it could be incorporated into the existing safety and security practices, namely the ISO 31000 risk management standard. The paper summarises the overall output of the IMPROVER project and my PhD project. It presents the framework in its final form, based on the iterative process in the IMPROVER project (workshop, pilot implementation, surveys, focus groups, feedback from operators). The paper address RQ1, RQ2, and RQ 3.

The paper starts by outlining the resilience discourse, focusing on the organisational, technological and societal domains of resilience. Here, we argue that resilience is needed, but that it should be integrated into the traditional risk thinking, not defending any school of thought. It goes on to present an approach to how the risk management standard can be extended to a CIR management framework. The paper then illustrates how the framework can be operationalised using one (of many possible) resilience assessment technique(s), namely CIRI, based on one of the pilot implementations in Barreiro.

In the paper, we strongly defend a plurality of techniques for CIR assessment, following the example of the ISO 31000 methodological approach on risk assessment (ISO, 2009b, 2019). In this paper, we have identified twelve CIR assessment techniques that are some of the most promising in the current context. Our review shows that they are usually based on a set of indices, which are then added in a simple cumulative way to form a holistic CIR index. While some remain simple typologies, others have been developed towards software application

already in use. The techniques differ considerably, especially in such issues as their selected domain of resilience, the required resources, ease of use, outcome in terms of quantitative or qualitative results, applicability of the results to create enhancement strategies, and so forth.

The article proposes a pre-standardisation input for the CIR management, tested in an operational environment. The article concludes with five maxims for this objective: no duplicate practices, tailorability, plurality of assessment techniques, measurability, and relative ease of use.

4.6 Paper VI

The aim of this paper is to identify the risk factors (observed and unobserved risk factors) affecting the recovery process of disrupted infrastructures. To this aim, the paper extends the application of accelerated failure time (AFT) models, which are used frequently in reliability engineering, to model the recovery time of disrupted CIs in the presence of unobserved and observed risk factors. The key novelty of the paper lies in exploring the application of AFT models in analysing the recoverability of disrupted infrastructures, in addition to analysing the impact of observed and unobserved risk factors on the recovery time. This is achieved by considering the operating conditions and other covariates, where the recovery time is selected to be the random variable of interest. The application and implications of the model are presented in a case study, from both a technical and a management perspective. The case study that is investigated in this paper applies the developed model, analysing recovery times from 73 disruption reports on Norwegian electric power distribution grids after four major extreme weather events. As the study show, certain covariates increase the recovery rate and improve recoverability, or, in other words, the recovery rate is higher under certain scenarios than others. The analysis indicates that failures in the regional grid, natural conditions, area affected, and failures in the operational control system have a significant impact on the recovery process. The results of the model analysis can be used to identify the parameters affecting the recovery process of infrastructure systems, providing the operator and regulator of the infrastructure with valuable information to improve both the technical systems and the organisational aspects of the infrastructure, in order to enhance the resilience level of the sociotechnical systems as a whole. In that way, they are better prepared for future events.

The paper contributes, to different degrees, to RQ 1, RQ 2 and RQ 3. The literature review and the analysis of the interruption data, justifies the need for CIR. The application of the statistical model contributes to the discussion on how resilience can be assessed. Finally, the implication of the results are discussed from a management perspective.

4.7 Paper VII

This paper reviews resilience analyses and assessments of real-life CIs in scientific publications. Although resilience of CIs has gained considerable attention in the research literature during the last decade, the underlying thesis here is that there remain relatively few resilience studies with application in real-life infrastructure, varying greatly in their operationalisation of the concept and with little guidance regarding concluding on the level of resilience of CIs. More concretely, we ask the questions: How is resilience operationalized, what methods are advocated for, are CI interdependencies addressed, and is it possible to conclude towards the resilience level of different CIs? Hence, the paper address RQ2 to a large

degree, and RQ1 and RQ3 to a minor degree. In general, the paper hence contributes to the research field by providing an overview of CIR resilience research, introducing the essence of research in the field to new researchers and providing a summarizing account of current research for active researchers.

Only a total of 50 scientific research articles were identified as relevant and subsequently reviewed, although using an open and systematic scoping approach and by utilizing the Scopus database. Only articles that explicitly stated to carry out resilience analyses of real-life infrastructures were included, although acknowledging that studies addressing for example vulnerability or recovery of infrastructures can be viewed as adding to the current state of knowledge regarding CI resilience. Associated concepts to resilience, such as robustness, reliability, survivability, rapidity, adaptation, and anticipation, is frequently used and it is explored how these are related to the concept of resilience. The approaches used for assessing CI resilience can be divided into four overarching groups: (1) empirical, (2) modelling and simulation, (3) expert, and (4) index or indicator approaches. The conceptualization of resilience varies across the articles, but where four fundamental resilience aspects can be discerned: anticipation, robustness, recovery, and adaptation. However, we conclude that most analyses tend to focus on only one or two resilience aspects simultaneously, where the clear majority focus either on robustness or recovery aspects. Only few of the reviewed articles suggests and analyse resilience enhancing measures, where most articles only conclude that the results are targeted towards such work. The overarching conclusion is that research regarding CI resilience of real-life infrastructures, and especially towards how to analyse and enhance CI resilience, is still in its infancy, where substantial efforts are needed towards being able to draw informed conclusions with respect to their level of resilience and the effect of interdependencies.

4.8 Contributions to research questions

The relationship between the papers and the research questions is illustrated in Table 11. Three + (+++) represent the highest correlation, while blank is the lowest.

Table 11. Contribution to research questions

Paper	RQ1	RQ2	RQ3
Paper I	+	++	+
Paper II	+	++	+
Paper III		+++	+
Paper IV	+	+++	++
Paper V	++	++	+++
Paper VI	+	++	+
Paper VII	+	+++	+

5 Results and discussion

Based on the seven appended papers, I here discuss and reflect on perspectives and key findings related to the three proposed research questions.

5.1 The need for CIR and its objectives

Resilience was introduced to me in 2015 when I started this project. Since then, I have tried to understand and utilise the concept. At the beginning, it was hard to grasp its meaning and comprehend why CIR is needed. Along the way, from both a theoretical and a methodological perspective, I have learned to see some clear benefits. Based on my papers and experience from the IMPROVER project, I will, at an overarching level, argue why there is need for CIR and what we are trying to achieve with CIR.

At the beginning of my project, I had an idea to investigate Arctic CIs, which Paper 1 clearly reflects. Later, and in conjunction with the IMPROVER project, I took a broader perspective, focusing not only on the Arctic region. However, in the first stage of my PhD project, some interesting viewpoint were brought up, being transferable to CIR in general. The paper highlights that extreme weather events in this region can be hard to predict, due to lack of data, and thus the operators of CIs in this region must have effective contingency plans, not only focusing on robustness and reliability, but also having a direct focus on recovery and restoration of infrastructures. Moreover, the lack of data works as a barrier to the practical application of the more traditional risk assessment approaches. Despite mentioning the UNISDR definition, I describe resilience as the sum of reliability and recoverability, excluding the more process-oriented attributes of resilience, such as anticipation and adaptation. In Papers II-V, I take a broader focus and use the UNISDR definition as the basis for describing resilience, stating that it can be seen as an umbrella concept in the CI context, including protection.

The various definitions of resilience are a good starting point to understand why CIR is needed. In Paper II, resilience is linked to the crisis management cycle, divided into seven phases, as illustrated in Figure 11. The first three phases (risk assessment, prevention, and preparedness) are often included in risk management. Hence, the resilience concept goes beyond traditional risk management and covers more than mere protection and pre-event capabilities. CIR is needed because complete protection of CIs can never be guaranteed. Moreover, achieving the

desired level of protection is normally not cost-effective in relation to actual threats. This view is also shared in European policy documents from mid-2010s onwards (see e.g. Pursiainen & Gattinesi, 2014) . A similar comparison can be made by using the performance loss function, as presented by Linkov et al. (2014) in Figure 12. A risk assessment determines the direct impact on the critical functionality of assets, depending on characteristics of threat, vulnerabilities and consequences, whereas resilience assessments take into account both pre-event planning, the direct impact, and the recovery process.

Figure 11. Seven resilience phases, inspired by the Crisis Management Cycle (Pursiainen, 2017)

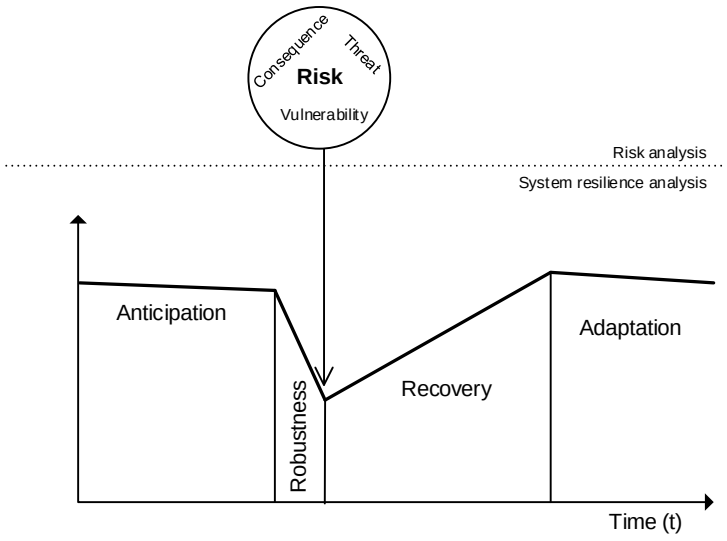

Figure 12. Risk vs. resilience. Adapted from Linkov et al. (2014)

This is a view that is shared by many CI operators. Through the IMPROVER project, six workshops were arranged, where CI operators were asked for their feedback through focus groups, questionnaires and surveys (IMPROVER Project, 2016d, 2018a, 2018b, 2018c; Petersen, Lange, et al., 2020). An overview of the workshops is presented in Table 7. In the same manner as in the academic community, the definition of resilience is contested among the operators. However, the operators believe that various definitions could also be a positive thing, and they do not see same need for a commonly agreed definition, as long as the objectives are clear. Moreover, some operators state that resilience is something that is already part of their organisation's daily activities, but it is not necessarily called resilience. In the same way as illustrated in Figure 11 and Figure 12, the operators stress that resilience goes beyond risk management. One important aspect here is that, compared to risk management, resilience also prioritises recovery time. This is also in line with the findings in the case study in Paper VI. Here, my study shows that the operators of the electricity grid in Norway acknowledge that it is impossible and not cost-effective to protect the system from everything, hence emphasising that there is a need for effective recovery plans and procedures as an integrated part of the existing risk management strategies. An essential component here is that these systems provide services to society in terms of supply of electricity – it is more important to maintain the service than protect the assets themselves. I contend that resilience is service-oriented rather than asset oriented. Moreover, considering the increasing complexities and interdependencies between CIs, it is very likely that unwanted events and surprises will occur. Hence, in the same way as Park, Seager, Rao, Convertino , and Linkov (2013), I claim that the resilience concept is adapted to cover these aspects, as prevention and mitigation are not always sufficient. The findings in the scoping study in Paper VII also validates this statement, where the majority of the articles take a broad perspective when conceptualising resilience, also including pre- and post-event aspects (e.g. anticipation and adaptation). However, as I will present in the next section, this is not always reflected in the analysis.

With the need for CIR justified, the next question is how to operationalise the concept. The feedback from many CI operators throughout the IMPROVER project was that the concept is already implemented (to some degree) but not necessarily framed as resilience. Thus, here – unlike in most of the previous literature – I will present methodologies for how resilience can be integrated in a formalised way into existing CI risk management. Simplified, I see this operationalisation process as twofold: first, finding suitable ways to measure and assess the resilience level; second, utilising the results to enhance resilience and improve CI performance over time as a continuous process. The overall aim is to present the results from my own studies but also to discuss them in conjunction with other existing operationalised approaches.

5.2 CIR assessment

5.2.1 Metrics, methods and techniques

As seen, there are myriads of different definitions of resilience. How resilience is measured will of course depend on how resilience is defined. This can be an obstacle when operationalising CIR assessments, at least in terms of comparability. Now, first, let us try to get an overview of the different resilience metrics.

Paper VII provides an overview of how CIR is measured and assessed in 50 scientific research articles, focusing on case studies in real-life infrastructure systems. Here, we distinguish

between six CIR metrics, or consequence types (with reference to the performance loss function), namely service, functional, topological, recovery, economic, and environmental. In short, this means the metric that can be used to measure the drop or loss in performance of the CI, indirectly or directly, referring to the consequence of the disruption. 'Functional' means that the metrics tries to capture the functionality of the infrastructure in terms of for example network oriented metrics such as largest connected subgraph or more engineering metrics such as loss of load. 'Service' is here used for metrics trying to capture the drop of service by the system such as customer or vital societal functions impacted. 'Recovery' are used for metrics trying to capture for example the time perspective of the interruption or demand on resources for recovery operation. 'Economic' are used when the metric described monetary consequence, and finally 'environmental' are used when the metric tries to capture the impact on the environment such as for example increased CO2-emissions. Furthermore, Paper VII goes on to categorise how the consequence metrics are used in conjunction with different methods (single, two or three methods), as seen in Table 12.

Table 12. Consequence metrics used in methods (results from scoping study in Paper VII)

	Methods(s)	**Consequence metrics**				
		Functional	Service	Recovery	Economic	Environ-mental
One	Network topological	[25],[31],[41],[44]	[2]	[14*]		
	Network flow	[20*],[32],[38]	[10*],[17*],[20*], [32],[47]		[47]	[47]
	Engineering		[1]			
	Dynamic economic	[16*]			[40]	
	Probabilistic	[4],[7]	[4],[28]	[7]	[7]	
	Statistical	[33*],[49]	[8*],[9*],[12], [21],[39]	[33*],[39],[49]		
	Expert elicitation					
	Surveys	[26]	[26]	[26]		
	System Dynamics	[3]			[3]	
	Discrete time model		[45]	[45]		
Two	Network topological & Network flow	[23*]	[23*]			
	Network topological & Probabilistic	[15*],[19*],[48]	[15*],[19*],[29*]		[15*]	
	Network topological & Expert elicitation			[18]		
	Network topological & Optimization	[43]	[43]			
	Network flow & Probabilistic	[6*],[34]	[34]			
	Network flow & Statistical		[5]			
	Network flow & Optimization	[24*]	[24*],[27]			
	Engineering & Monte-Carlo	[30]		[30]		
	Dynamic economic & Statistical	[46*]				
	Probabilistic & Expert elicitation	[35]				
	Statistical & Surveys		[37]			
	Expert elicitation & Surveys	[11*]	[11*]			
Three	Network topological, Expert elicitation & Monte-Carlo			[13]		
	Network flow, Engineering & Optimization	[42]				
	Network flow, Static economic & Surveys		[50*]			
	Probabilistic, Expert elicitation & Surveys		[22*]			

These methods are linked to the four broader assessment approaches presented in Table 5. As seen in Table 12 'functional' and 'service' are the most frequently used metric, followed by recovery. Most articles use several methods and consequence metrics in combination. Studies that address interdependencies are marked with a star (*) in superscript.

I now go on to present the CIR assessment methods and techniques for CIR assessment, developed in this study. It is worth noting that one specific assessment technique can use several methods.

In Paper I, I claim that the most important factors to take into consideration when quantifying the resilience of Arctic infrastructures are (i) reliability of infrastructure components, (ii) supportability of disrupted components, (iii) maintainability of disrupted elements, (iv) resilience of the owner's organisation in the case of disruption, and (v) the prognostics and health management (PHM) efficiency of the system. Reliability quantifies the ability of the infrastructure to maintain its capacity and performance above an acceptable limit during a given period under given conditions. The four latter components influence the recoverability of the infrastructure. Recoverability measures the ability of the infrastructure system to restore its capacity and performance by recovering from the adverse effects of adverse events during a period of time, under given conditions, using the available resources. Recoverability can be a non-linear function of system reliability, indicating that the performance of recovery action is affected by the health of the infrastructure. Based on these factors, inspired by Youn et al. (2011), resilience at time *t* can be formulated as:

$$\Psi_j(t) = R_j(t) + \Lambda_j(t) \cdot \left(1 - R_j(t)\right) \tag{2}$$

where R_j is the reliability of the infrastructure, and Λ_j is the product of organisational resilience, maintainability, PHM efficiency, and supportability. The organisational component is included to address the linkage between physical infrastructure systems and the social system. However, how to quantify organisational resilience is not properly addressed in this paper and is better reflected in some of my other contributions. Furthermore, the paper goes on to describe a step-by-step guideline for how to calculate the infrastructure resilience using this formulation, by using statistical methods and/or expert judgements. In the paper, it is highlighted that to use statistical methods, repair and failure data should be available, associated with their risk factors, such as ambient temperature, number of repair crew, active repair time, etc. This is not properly addressed in this paper; however, Paper VI considers these factors. These risk factors can broadly be categorised into two different groups, namely observed and unobserved risk factors. In most studies on resilience, the effect of unobserved covariates is neglected. Paper VI extends the application of accelerated failure time (AFT) models, to model the recovery time of disrupted CIs in the presence of unobserved and observed risk factors.

To better capture organisational factors, Paper II proposes an index method to assess CIR, namely the Critical Infrastructure Resilience Index (CIRI). CIRI integrates indicators from both the technological and organisational domains. CIRI classifies indicators under the seven crisis management cycle phases, as presented in Figure 11, describing the temporal dimensions of resilience. These seven phases are referred to as resilience phases at Level 1, further broken down into components and processes at Level 2, generic indicators at Level 3, and finally-

sector-specific and actually addressed indicators at Level 4. Level 4 indicators are measured first, and the measurement accumulates upwards through the scaling process, producing comparable results. The scoring of indicators is carried using a semi-quantitative maturity scale inspired by COBIT 4.1 (Control Objectives for Information Technologies (COBIT), 2007). The output from CIRI is either an overall resilience index, representing the accumulated resilience with a maturity scale value, or a breakdown of the maturity in the different phases. The results are presented in radar charts. Figure 13 presents the overall CIRI structure.

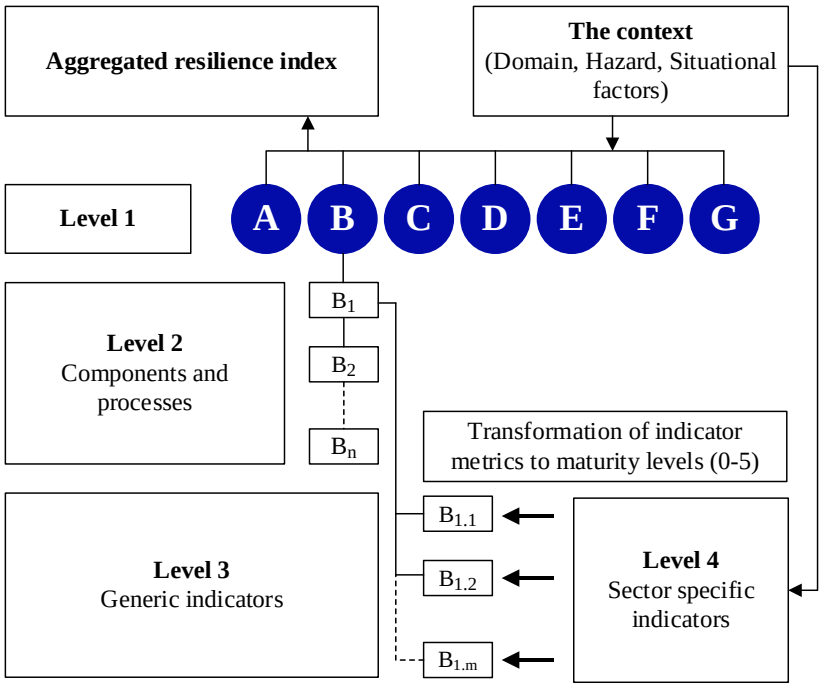

Figure 13. CIRI overall scheme

In Paper III, to provide a comparable perspective, two other methods/techniques are presented in conjunction with CIRI. These are the Benchmark Resilience Tool (BRT) (Lee et al., 2013) and Guidelines for Critical Infrastructure Resilience Evaluation (CIRE) (Bertocchi et al., 2016). Both techniques are expert- and index-based, and use indicators to measure resilience. BRT only considers the organisational domain.

In Paper IV, CIRI and two other IMPROVER-developed assessment techniques are presented: IMPROVER Organisational Resilience Analysis (IORA) and IMPROVER Technological Resilience Analysis (ITRA). As the names indicate, these techniques are tailored for one specific resilience domain, while CIRI is considered to be holistic (considering more than one CIR domain). IORA is process-oriented and provides only qualitative assessments. ITRA uses engineering methods to model and simulate the actual performance of the CI, in terms of service level.

Paper V compares twelve different assessment techniques, including some of the techniques presented in this section. The techniques are not ranked, but to put them into a comparable perspective, several attributes are used to identify their differences, such as resource and capability, uncertainty, complexity, ability to provide quantitative output, and resilience domain covered. The overview of the techniques are shown in Appendix A in Paper V. The

scoping study in Paper VII did not identify these assessment techniques, implying that they most likely have not been applied in a real-life environment.

5.2.2 Application and implementation

Based on my study, I will now go on to present how to apply and implement these metrics, methods and techniques for CIR assessment to real-life CIs. I also discuss the concrete results from the assessments.

Through the IMPROVER project, several assessment techniques have been demonstrated and implemented, including CIRI, ITRA and IORA. Paper III evaluates CIRI and two other techniques (BRT and CIRE), by applying them in a desk-top demonstration. The study shows that all techniques have pros and cons. All the techniques end up quantifying the resilience with a final score. However, what the score actually means is dependent on the interpretation of the end-user, and there is no clear guidance on how the results should be used to enhance the resilience level. This feedback was further taken into account for the IMPROVER pilot implementations, where CIRI, ITRA and IORA were applied. Before the pilot implementation, in cooperation with the CI operators, an initial demonstration applied all the techniques. The structure and processes of the resilience assessment techniques proved functional in the demonstrations. However, the operator brought up a few issues, such as user-friendliness, the fact that assessments should be clear and not too complex, the crucial role of resilience indicators in the monitoring of resilience activities, the importance of ensuring objectivity, and the fact that consistency and repeatability create representative results. The operators highlighted that, as long as the indicators are well described and leave little room for subjectivity, the high number of indicators is not a problem. Moreover, they emphasise the need for clear guidelines and defined measurement scales for indicators.

The assessment results from CIRI in the pilot implementation indicated that the operator should prevent silos (i.e. to have quick and easy cooperation between management and people in the field) and have structures in place to ensure this. Adjustment from initial demonstrations made the indicators easier to interpret. The implementation also shows that different resilience assessment techniques have the ability to bring up different levels of details and different perspectives. For instance, IORA identifies that silo-preventing mechanisms already exist in the organisation, albeit as an unofficial way of working.

In Paper VI, the developed AFT model is applied to historical interruption data from the Norwegian electricity grid, in order to analyse the recoverability of the grid and to identify and analyse the effect of risk factors. The analysis indicated that failure in the regional grid, natural conditions, area affected, and failures in operational controls systems have a significant impact on the recovery process. The model proved to be useful, and analysis results can provide the grid operators and regulator with valuable information to improve both the technical systems and the organisational aspects of the infrastructure, in order to enhance the resilience level of the socio-technical system as a whole. However, using this model requires a high level of competence, calling for the need for external expertise. Moreover, to produce reliable results, more data is needed to rerun and validate the model.

Paper VII presents an overview of academic peer-reviewed literature that applies methods on real-life infrastructures to assess their resilience. As earlier discussed, the majority of the

articles takes a broad perspective when they define and conceptualise resilience. However, this is, a bit surprisingly, seldom reflected in the analysis part of the articles. The analysis normally take a narrower focus, concentrating on robustness and recovery only. The results further revealed that many concepts are used in conjunction with resilience and that many studies aim for resilience analysis, but then fall back to more conventional concepts such as vulnerability, reliability and robustness. This is connected to the fact that many of the studies take a narrower focus in their resilience analysis, compared to their conceptual definition. The same trend is found in terms of methods and approach used, where there seems to be no single analysis method that manage to capture all dimensions and aspects of resilience. This indicated that – in spite of the growth in the demand of research on CIR analysis and assessment methodologies – the innovative potential of resilience as a concept is not fully utilised in current applied literature. Moreover, as the results of the study show, most articles focus on hazards and treats that CIs are frequently exposed to. Hence, it is difficult to tell to what level CIs are also resilient towards more low probability events and against new and emerging threats. For instance, we found no studies that consider cyber terrorism, tornado, lightning, sabotage, and pandemic – which potentially could cause significant losses in performance. This finding add an interesting perspective to the debate whether resilience is dependent on detailed hazard scenarios or not (Aven, 2016, 2019; Cutter, 2016). The reason for this could be associated with the conceptual approaches being used. It seems like conventional 'risk-thinking' is still prevalent in the studies, with the tendency of excluding surprising and rare events.

The scoping study also reveals there are many CIs that are not addressed in the identified literature, such as fuel supply, seaports, satellite systems, and agriculture. Food supply is only considered in one of the articles. The majority of the articles considers electricity, transportation and waste & water infrastructures. The reason for this could be that operators of these CIs have better procedures for collecting and recording data as indicated by Johansson, Jonason Bjärenstam , and Axelsdóttir (2018). Moreover, quite surprisingly, most of the articles considers CIs on local and regional spatial levels, and very few at a national and cross-border spatial levels. At international level, the only infrastructure studied is the air traffic infrastructure. This could also be linked to data collection barriers and the sensitive nature of the data, especially at cross-border spatial levels.

As there are no strictly objective way to evaluate and compare these CIR assessment methodologies and techniques, my claim, therefore, is that much will depend on what one wants do with a resilience assessment technique, the amount of effort and time available, and who is doing it. In general, it is important that a technique provides a transparent and repeatable work process, with results that are verifiable, and is applicable at least for organisational and technological CIR assessments. Furthermore, as stated by the operators, it is crucial that such techniques can create comparable results, in order to facilitate enhancement of resilience over time. This central component of an assessment, namely evaluation of the results, is an area with potential for improvement. The review study in Paper VII put forward evidence to that effect. The majority of the 50 case studies identified and reviewed does not provide any conclusion on the resilience level at all. Moreover, there are few studies that address and analyse resilience building measures (i.e. how to enhance resilience), with the most studies only concluding that the results are targeted towards such work. Hence, more efforts should be directed towards developing clear resilience evaluation methods.

5.3 CIR management

In this section, I will present the final proposed CIR management framework that is compatible with existing risk management practices, as presented in Paper V, bringing all the pieces together. The approach is based on mapping CIR against definitions and concepts already used in risk management in the ISO 31000 international standard (ISO, International Organization for Standardization (ISO), 2009a; 2018). As I allege, the approach has an advantage in that many organisations are already familiar with the standard. However, criticisms have been raised against ISO 31000 within the risk research community. The original 2009 standard was claimed to be unclear, leading to illogical decisions if followed, impossible to comply with, and not mathematically based, having little to say about probability, data and models (Aven, 2011; Leitch, 2010). By the same token, the revised 2018 version was criticised for its lack of scientific grounding and for being inconsistent (Aven & Ylönen, 2019).

I partly agree with this criticism, but my claim is that the most important achievement of the ISO 31000 standard is its approximation of terminology and its understanding of the basic framework of risk management processes among practitioners. Despite its shortcomings, the standard has improved the generic risk management level in many organisations. As Aven (2016) states, the standard basic structure is used "in most risk analysis textbooks" (p. 6), in addition to being applied on a daily basis in companies (Aven & Ylönen, 2019) and by international organisations such as the EU (European Commission, 2017), OECD (2014), and the UNDRR (2017).

To my mind, these pragmatic arguments justify the effort towards a CIR management framework that is aligned with existing practice, rather than developing a completely new scheme that would probably lead to a great deal of resistance from practitioners. I see ISO 31000 as an opportunity to introduce and formalise CIR practices in the field. This is also consistent with the feedback from operators in the IMPROVER project; as one of the operators in one workshop stressed: "We don't have to reinvent the wheel [to be resilient]" (Petersen et al.,2020, p. 5).

ISO 31000 divides risk management into several stages, including 'setting the scope, context and criteria', 'risk assessment', and 'risk treatment', in addition to the cross-cutting functions of 'communication and consultation' and 'monitoring and review' through all of the steps. Risk assessment consists of risk identification, risk analysis and risk evaluation. Based on the risk evaluation, the risk treatment phase comprises measures to prevent or mitigate the risk. The framework I present enhances the current risk management practices by adding the CIR component. While risk management has a stronger focus on pre-event characteristics, CIR management emphasises preparedness, response and the rapidity of recovery applied during and after the event.

The components of the CIR management framework are described as follows:

CIR management	The name for all the coordinated activities undertaken to direct and control an organisation with regard to its resilience, including the processes below.

Setting the scope, context and criteria	The first phase of CIR management. It entails identifying the criteria for the subsequent analysis and evaluation, such as time window and other basic parameters, as well as perceived societal tolerance levels or minimum quality/quantity of service performance for a community to survive.
CIR analysis	The process of determining the level of resilience with one or more appropriate technique.
CIR evaluation	The process of comparing the results of a CIR analysis with selected criteria, to determine whether the level of resilience is acceptable and to identify priority areas for further enhancement.
CIR enhancement	The process of developing and implementing plans for improving resilience, for example by focusing on the absorptive, adaptive or restorative capacity. The enhancement will change the input into the whole process, making CIR management an iterative activity that needs to be constantly revisited by the organisation.

Against this backdrop, Figure 14 presents the framework for parallel and interlinked CI risk management and resilience management.

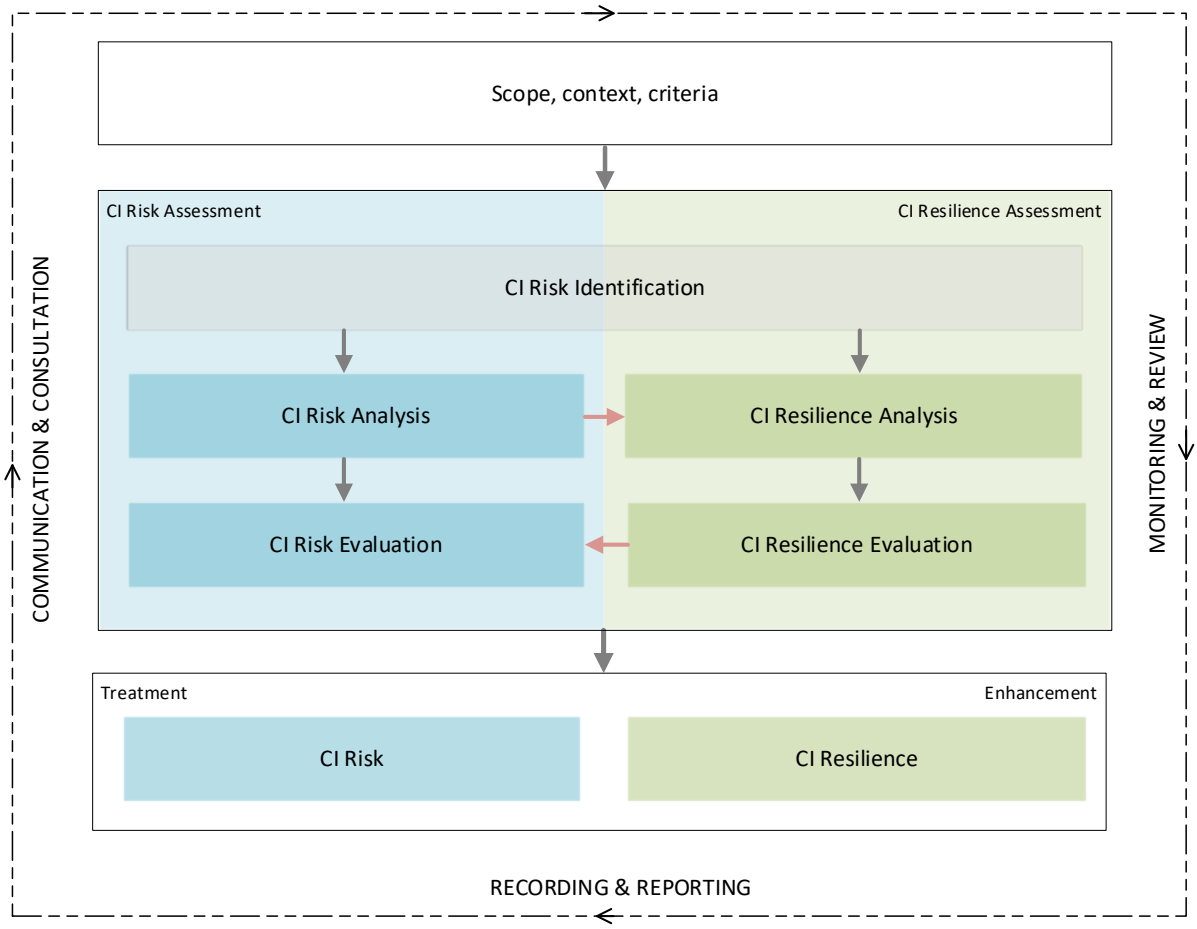

Figure 14. The overall CIR management framework

Risk identification here feeds into the CIR assessment (analysis and evaluation), also taking into account threats, hazards and scenarios that are excluded in a traditional risk assessment. Risk assessments provide important input for the CIR assessment, by supplying information about the impact and the vulnerability of the CI to specific hazards. On the other hand, CIR analysis feeds back into the risk management process. The output of the overall framework supersedes a mere CI risk treatment plan, also including a holistic CIR enhancement plan. As the scoping study in Paper VII shows, many of these key components are missing or underdeveloped in current applications to real-life infrastructures, especially CIR evaluation and enhancement.

As presented in Section 5.2, there are numerous methods and techniques used to measure and assess resilience. The proposed framework defines the main concept and goals of CIR management, but I claim that such a framework should not define the exact techniques and methods for reaching these goals. Too strict definitions are known to hinder creative developments, yet they should provide guidance (Aven & Ylönen, 2019; Brunsson, Rasche, & Seidl, 2012; Timmermans & Epstein, 2010). Rather effective guidelines already exist on how to select risk assessment techniques (ISO, 2009b, 2019). Similar guidance should be provided for choosing between the different CIR assessment techniques. In general, the decision on which technique(s) to use for CIR assessment should be taken in relation to setting the scope, context and criteria. Any relevant technique could be used, depending on the objective, needs and requirements, level of ambiguity, information and data availability, and resources of the organisation carrying out the assessment. Furthermore, it is advantageous that the results obtained from the risk analysis are transferable to the CIR assessment and vice versa.

I contend that a CIR assessment technique should provide a transparent and repeatable work process, with results that are verifiable, and applicable for organisational and technological CIR assessment. As stated in the previous section, in Appendix 1 in Paper V, some of the available techniques, including techniques developed in the IMPROVER project (Paper II-IV) are presented and compared against certain attributes, aligned with the ISO 31000 practice. These techniques and other techniques and methods presented in the previous section, could be applied in the proposed framework, depending on the needs and objectives of the operator.

In many ways, with the aforementioned framework, I outline how one could standardise and operationalise CIR management in a systematic manner. Of course, I do not see this as a definitive solution, and the path towards an approved and acknowledged CIR standard is long. It took years to agree on the ISO 31000 standard, both the 2009 and 2018 editions, and the same will probably be the case for CIR. However, to that effect, some serious efforts are being made, both nationally and internationally, for instance at the European Union level, with several resilience projects and approaches, including IMPROVER, joining forces (White Paper, 2018). With respect to these efforts and to conclude this chapter, I put forward five maxims for successful CIR management.

First, there should be *no duplicate practices*. The experience from this PhD project is that CI operators and owners, mostly profit-seeking organisations, while having a self-interest in enhancing their CIR, do not want to change their systems overnight when the scientific discourse changes. To that end, I defend and present a CIR management system that is compatible with the operator's current risk management (RM) systems and procedures.

Second, a CIR management system should be *tailorable*. As my study has shown, no framework or standard, should be too rigidly defined. The development of the ISO 31000 RM standard substantiates this argument. The original version of the ISO 31000 RM standard is much more detailed than the 2018 version. This change was made because sectors, companies and organisations do not see the need for too well-defined and detailed frameworks, but they do need some kind of framework to tailor their needs.

Third, I contend that a *plurality of techniques and methods* is needed. As this study shows, there is no single approach, method or technique that would provide all the answers for all sectors, conditions, situations, needs or resources for a risk or CIR assessment.

Fourth, I claim that any CIR management system should be based on *measurability*. In order to evaluate, compare, monitor, and enhance resilience, it is essential to have well-defined indicators or other performance metrics. Without such measurement, my assertion is that CI operators would be in the dark about what and how much to enhance.

Fifth, as this thesis shows, CIR management is multifaceted and complex, hence calling for increased professional skills and resources. Nevertheless, CIR management should be characterised by relative *ease of use*, preferably computable. As the operator clearly sees the need for CIR, and it is too important for any operator to subcontract, the system should be such that it is easy to integrate into the daily activities of the organisations concerned.

6 Conclusion

6.1 Research conclusions

In this thesis, I have contributed valuable knowledge and insight to the CIR field, at both a conceptual and a methodological level.

Based on a review of existing literature and practices, and experience from my study, I provide a justification for why CIR is needed, and present what we would like to achieve with the concept. Most importantly, CIR goes beyond traditional risk management and covers more than pre-event capabilities, because protection of CIR can never be guaranteed.

I further go on to present the developed methods and techniques for measuring and assessing CIR – evaluated, demonstrated, and implemented in a real-life environment. These are discussed in a comparative perspective in conjunction with other existing approaches. I defend the plurality of techniques and methods and emphasise the need for measurability and comparability. As my study shows, there is no single approach, method or technique that would provide all the answers for all sectors, conditions, needs or resources for a CI risk and resilience assessment.

Finally, at an overarching level, I present a way in which CIR management can be conceptualised, operationalised and methodologically enhanced. I have put forward evidence that this could be achieved by utilising the often-used practices of risk management, thus modifying the current international management standard towards that of CIR management. To this end, I present a framework that closely follows the standardised risk management typology, but adapted to CIR. This framework facilitates the plurality of assessment methods and techniques. To summarise, I conclude with five maxims for successful CIR management: no duplicate practices; tailorability and plurality of assessment techniques and methods; measurability; and relative ease of use.

6.2 Future research

This study has identified several research gaps related to CIR, which opens the door for future research opportunities.

Methodologically, there are hardly any single assessment methods or techniques that manage to capture all the aspects of resilience; instead, there seems to be a need to combine several methods. The question is whether research should aim to develop such a single method, considering the multifaceted CIR concept, and whether this is at all possible. Moreover, the latter part of a CI resilience assessment, namely evaluation, seems to be largely under-researched. This especially applies to comparing the CI performance against the public's tolerance levels.

With respect to assessment of real-life infrastructures, this study also reveals the sparse completeness of the type of infrastructure addressed, hazards included and spatial level of the analyses. Hence, more research regarding CI resilience of real-life infrastructures are needed to form future policies, and especially toward how to analyse and enhance CI resilience, where substantial efforts are need towards being able to draw informed conclusion with respect to their level of resilience and the effect of interdependencies.

To potentially standardise the proposed CIR management framework, I see a clear need to further test, demonstrate and implement the framework in a real-life environment.

Bibliography

Adger, W. N. (2003). Building resilience to promote sustainability, Newsletter published by The International Human Dimensions Programme on Global Environment Change. Bonn, Germany, *IHDP Update*, 02/2003, pp. 1-3.

Akter, M. N., Nasiruzzaman, A., Mahmud, M. A., & Pota, H. R. (2014). *Topological resiliency analysis of the Australian electricity grid with increased penetration of renewable resources*. Paper presented at the 2014 IEEE International Symposium on Circuits and Systems (ISCAS), Melbourne, Australia.

Aldrich, D. P., & Meyer, M. A. (2015). Social capital and community resilience. *American Behavioral Scientist, 59*(2), 254-269.

Alexander, D. E. (2013). Resilience and disaster risk reduction: An etymological journey. *Natural Hazards and Earth System Sciences Discussions, 1*(2), 1257-1284.

Aligne, F., & Mattioli, J. (2011). The role of context for crisis management cycle. In F. Burstein, P. Brezillon, & A. Zaslavsky (Eds.), *Supporting real time decision-making* (Vol. 13, pp. 113-132). Boston, US.: Springer.

Allen, P. M., Datta, P. P., & Christopher, M. (2006). Improving the resilience and performance of organizations using multi-agent modelling of a complex production–distribution systems. *Risk Management, 8*(4), 294-309.

American National Standards Institute (ANSI). (2009). *Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for Use.* (ANSI/ASIS.SPC.1:2009.). Available from https://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf.

Arksey, H., & O'Malley, L. (2005). Scoping studies: Towards a methodological framework. *International journal of social research methodology, 8*(1), 19-32.

Aven, T. (2011). On the new ISO guide on risk management terminology. *Reliability engineering & System safety, 96*(7), 719-726.

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

Aven, T. (2019). The call for a shift from risk to resilience: What does it mean? *Risk Analysis, 39*(6), 1196-1203.

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.

Barabadi, A., & Ayele, Y. (2018). Post-disaster infrastructure recovery: Prediction of recovery rate using historical data. *Reliability Engineering & System Safety, 169*, 209-223.

Barabadi, A., Barabady, J., & Markeset, T. (2011). Maintainability analysis considering time-dependent and time-independent covariates. *Reliability Engineering & System Safety, 96*(1), 210-217.

Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. *Reliability Engineering & System Safety, 117*, 89-97.

Benson, C., Twigg, J., & Rossetto, T. (2007). *Tools for mainstreaming disaster risk reduction: Guidance notes for development organisations*. Geneva, Switzerland: ProVention Consortium.

Bergström, J., Van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety, 141*, 131-141.

Berkes, F., & Jolly, D. (2002). Adapting to climate change: Social-ecological resilience in a Canadian western Arctic community. *Conservation Ecology, 5*(2).

Bertocchi, G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A., . . .Traballesi, A. (2016). *Guidelines for Critical Infrastructures Resilience Evaluation*. Rome, Italy:

Associazione Italiana esperti Infrastrutture Critiche (AIIC) – Italian Association of Critical Infrastructures Experts. DOI: 10.13140/RG.2.1.4814.6167

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: the concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375-5393.

Boin, A., & McConnell, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. *Journal of Contingencies and Crisis Management, 15*(1), 50-59.

Boon, H. J., Cottrell, A., King, D., Stevenson, R. B., & Millar, J. (2012). Bronfenbrenner's bioecological theory for modelling community resilience to natural disasters. *Natural Hazards, 60*(2), 381-408.

Braes, B., & Brooks, D. (2010). *Organisational resilience: A propositional study to understand and identify the essential concepts.* Paper presented at the 3rd Australian Security and Intelligence Conference, 30th November 2010, Edith Cowan University, Perth Western Australia.

British Standard (BS). (2014). *Guidance on organizational resilience* (BS 65000:2014). London, United Kingdom.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., . . .Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra, 19*(4), 733-752.

Brunsson, N., Rasche, A., & Seidl, D. (2012). The dynamics of standardization: Three perspectives on standards in organization studies. *Organization Studies, 33*(5-6), 613-632.

Burgess, R. (1984). In the field: An introduction into field research. *George Allen & Unwin, London. Burgleman RA (1983) Internal corporate Venturing, Administrative Science Quarterly, 28*, 223-244.

Burnard, K., & Bhamra, R. (2011). Organisational resilience: development of a conceptual framework for organisational responses. *International Journal of Production Research, 49*(18), 5581-5599.

Chang, S. E., McDaniels, T., Fox, J., Dhariwal, R., & Longstaff, H. (2014). Toward disaster - resilient cities: Characterizing resilience of infrastructure systems with expert judgments. *Risk Analysis, 34*(3), 416-434.

Chang, S. E., & Shinozuka, M. (2004). Measuring improvements in the disaster resilience of communities. *Earthquake spectra, 20*(3), 739-755.

Chopra, S. S., Dillon, T., Bilec, M. M., & Khanna, V. (2016). A network-based framework for assessing infrastructure resilience: A case study of the London metro system. *Journal of The Royal Society Interface, 13*(118), 20160113.

Control Objectives for Information Technologies (COBIT). (2007). *Excerpt. Executive Summary Framework.* IT Governance Institute. Available from http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/cobit-4-1.aspx.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice, 39*(3), 124-130.

Crichton, M. T., Ramsay, C. G., & Kelly, T. (2009). Enhancing organizational resilience through emergency planning: Learnings from cross - sectoral lessons. *Journal of Contingencies and Crisis Management, 17*(1), 24-37.

Cutter, S. L. (2016). The landscape of disaster resilience indicators in the USA. *Natural hazards, 80*(2), 741-758.

Cutter, S. L., Barnes, L., Berry, M., Burton, C., Evans, E., Tate, E., & Webb, J. (2008). A place-based model for understanding community resilience to natural disasters. *Global Environmental Change, 18*(4), 598-606.

Daudt, H. M., van Mossel, C., & Scott, S. J. (2013). Enhancing the scoping study methodology: A large, inter-professional team's experience with Arksey and O'Malley's framework. *BMC medical research methodology, 13*(1), 48.

De Bruijne, M., Boin, A., & Van Eeten, M. (2010). Resilience: Exploring the concept and its meanings. In L. K. Comfort, A. Boin, & C. C. Demchak (Eds.), *Designing resilience: Preparing for extreme events* (pp. 13-32). Pittsburgh, USA: University of Pittsburgh Press.

Denzin, N. K. (1978). Triangulation: A case for methodological evaluation and combination. Introduction. In N. K. Denzin (Ed.), *Sociological methods. A sourcebook*. New York: MacGraw-Hill.

Denzin, N. K., & Lincoln, Y. S. (2011). *The Sage handbook of qualitative research*. California, USA: Sage Publications.

Deverell, E., & Olsson, E.-K. (2010). Organizational culture effects on strategy and adaptability in crisis management. *Risk Management, 12*(2), 116-134.

Djalante, R., Holley, C., & Thomalla, F. (2011). Adaptive governance and managing resilience to natural hazards. *International Journal of Disaster Risk Science, 2*(4), 1-14.

Dovers, S. R., & Handmer, J. W. (1992). Uncertainty, sustainability and change. *Global Environmental Change, 2*(4), 262-276.

Dresch, A., Lacerda, D. P., & Antunes, J. A. V. (2015). Design Science Research. In A. Dresch, D. P. Lacerda, & J. A. V. Antunes (Eds.), *Design Science Research* (pp. 67-102). Cham, Switzerland: Springer International Publishing.

Espinoza, S., Panteli, M., Mancarella, P., & Rudnick, H. (2016). Multi-phase assessment and adaptation of power systems resilience to natural hazards. *Electric Power Systems Research, 136*, 352-361.

European Commission. (2005). *Green paper on a European Programme for Critical Infrastructure Protection* (COM(2005) 576 final). Brussels, Belgium. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN.

European Commission. (2013). *Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Infrastructures more secure.* (SWD(2013) 318 final). Brussels, Belgium. Available from https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf.

European Commission. (2017). *Commission Staff Working Document on Overview of Natural and Man-made Disaster Risks the European Union may face* (SWD(2017) 176 final). Brussels, Belgium. Available from https://ec.europa.eu/echo/sites/echo-site/files/swd_2017_176_overview_of_risks_2.pdf.

European Commission. (2019). *Commission staff working document. Evaluation of Council Directive 2008/114 On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* (SWD(2019) 308 final). Brussels, Belgium. Available from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf.

Field, C. B., Barros, V., Stocker, T. F., & Dahe, Q. (2012). *Managing the risks of extreme events and disasters to advance climate change adaptation: Special report of the intergovernmental panel on climate change*: Cambridge University Press.

Fiksel, J. (2006). Sustainability and resilience: Toward a systems approach. *Sustainability: Science, Practice and Policy, 2*(2), 14-21.

Flach, P. A., & Kakas, A. C. (2000). Abductive and inductive reasoning: Background and issues. In P. A. Flach & A. C. Kakas (Eds.), *Abduction and induction. Applied Logic Series* (Vol. 18, pp. 1-27). Dordrecht, Netherlands: Springer.

Fletcher, D., & Sarkar, M. (2013). Psychological resilience: A review and critique of definitions, concepts, and theory. *European Psychologist, 18*(1), 12.

Flint, C. G., & Luloff, A. E. (2007). Community activeness in response to forest disturbance in Alaska. *Society and Natural Resources, 20*(5), 431-450.

Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. *Global Environmental Change, 16*(3), 253-267.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety, 121*, 90-103.
Geis, D. E. (2000). By design: The disaster resistant and quality-of-life community. *Natural Hazards Review, 1*(3), 151-160.
Gibson, C. A., & Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience. *Australian Journal of Emergency Management, 25*(2), 6.
Giroux, J., & Prior, T. (2012). *Expression of Resilience: From "Bounce back" to Adaptation* (3RG REPORT Factsheet). Zurich, Switzerland. Available from https://www.files.ethz.ch/isn/170633/Factsheet-Expressions-of-Resilience.pdf: Center for Security Studies (CSS), ETH Zurich.
Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report, 8*(4), 597-607.
Gundel, S. (2005). Towards a new typology of crises. *Journal of contingencies and crisis management, 13*(3), 106-115.
Handmer, J. W., & Dovers, S. R. (1996). A typology of resilience: Rethinking institutions for sustainable development. *Industrial & Environmental Crisis Quarterly, 9*(4), 482-511.
Hevner, A., & Chatterjee, S. (2010). *Design research in information systems: Theory and practice* (Inegrated Series in Information Systems Vol. 22). Boston, USA: Springer Science & Business Media.
Hevner, A., March, S. T., Park, J., & Ram, S. (2004). Design science research in information systems. *MIS Quarterly, 28*(1), 75-105.
Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*(1), 1-23.
Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate Publishing Ltd.
Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety, 145*, 47-61.
Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288.
Hughes, T. P., Baird, A. H., Bellwood, D. R., Card, M., Connolly, S. R., Folke, C., . . .Kleypas, J. (2003). Climate change, human impacts, and the resilience of coral reefs. *Science, 301*(5635), 929-933.
Ibbs, W., & Nguyen, L. D. (2007). Alternative for quantifying field-overhead damages. *Journal of Construction Engineering and Management, 133*(10), 736-742.
IMPROVER Project. (2016a). *Final lexicon of definitions* (Deliverable 1.3). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2016b). *International Survey* (Deliverable 1.1). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2016c). *Report of criteria for evaluating resilience* (Deliverable 2.2). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2016d). *Report of operator workshop 1* (Deliverable 1.4). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2016e). *Social resilience criteria for critical infrastructures during crises* (Deliverable 4.1). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2017). *Technological resilience concepts applied to critical infrastructure* (Deliverable 3.2). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2018a). *Report from associate partner workshops* (Deliverable 1.7). Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2018b). *Report of operator workshop 2*. Available from http://improverproject.eu/category/results/.
IMPROVER Project. (2018c). *Report of operator workshop 3* (Deliverable 1.6). Available from http://improverproject.eu/category/results/.
International Organization for Standardization (ISO). (2009a). *Risk management -- Principles and guidelines* (ISO 31000:2009). Geneva, Switzerland.

International Organization for Standardization (ISO). (2009b). *Risk management -- Risk assessment techniques* (IEC/FDIS 31010). Geneva, Switzerland.

International Organization for Standardization (ISO). (2011). *Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use.* (ISO 28002:2011). Geneva, Switzerland.

International Organization for Standardization (ISO). (2014a). *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations* (ISO 28000-2:2011). Geneva, Switzerland.

International Organization for Standardization (ISO). (2014b). *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 3: Additional specific guidelines for adopting ISO 28000 for use of medium and small businesses (other than marine ports)* (ISO 28004-3:2014). Geneva, Switzerland.

International Organization for Standardization (ISO). (2014c). *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 4: Additional specific guidelines for adopting ISO 28000 if compliance with ISO 280001 is a management objective* (ISO 28004-4:2014). Geneva, Switzerland.

International Organization for Standardization (ISO). (2017). *Security and resilience — Guidelines for organizational resilience* (ISO/DIS 22316). Geneva, Switzerland.

International Organization for Standardization (ISO). (2018). *Risk management – Guidelines.* (ISO 31000:2018). Geneva, Switzerland.

International Organization for Standardization (ISO). (2019). *Risk management - Risk Assessment techniqies* (IEC 31010:2019). Geneva, Switzerland.

Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering & System Safety, 95*(12), 1335-1344.

Johansson, J., Jonason Bjärenstam, R., & Axelsdóttir, E. (2018). Contrasting critical infrastructure resilience from Swedish infrastructure failure data. In S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik, & J. E. Vinnem (Eds.), *Safety and Reliability–Safe Societies in a Changing World: Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway*. London, UK: Taylor and Francis Group.

Jordan, T., & Alcantara, P. (2014). *Conceptualising organisational resilience* (Business Continuity Institute Working Paper Series). Business Continuity Institute Research Department. Caversham, UK. Available from http://static.ow.ly/docs/BCIWorkingPaper3_2JOq.pdf.

Kahan, J. H., Allen, A. C., & George, J. K. (2009). An operational framework for resilience. *Journal of Homeland Security and Emergency Management, 6*(1).

Kameshwar, S., Cox, D. T., Barbosa, A. R., Farokhnia, K., Park, H., Alam, M. S., & van de Lindt, J. W. (2019). Probabilistic decision-support framework for community resilience: Incorporating multi-hazards, infrastructure interdependencies, and resilience goals in a Bayesian network. *Reliability Engineering & System Safety, 191*, 106568.

Kimchi, J., Polivka, B., & Stevenson, J. S. (1991). Triangulation: operational definitions. *Nursing Research, 40*(6), 364-366.

Kotzanikolaou, P., Theoharidou, M., & Gritzalis, D. (2011). Interdependencies between critical infrastructures: Analyzing the risk of cascading effects. In S. Bologna, B. Hämmerli, D. Gritzalis, & S. Wolthusen (Eds.), *Critical Information Infrastructure Security. CRITIS 2011* (pp. 104-115). Lecture Notes in Computer Science, vol 6983: Springer, Berlin, Heidelberg.

Kozine, I., & Andersen, H. B. (2015). *Integration of resilience capabilities for critical infrastructures into the emergency management set-up.* Paper presented at the European Safety and Reliability Conference 2015, Zurich, Swizerland.

Kudo, Y., Murai, T., & Akama, S. (2009). A granularity-based framework of deduction, induction, and abduction. *International journal of approximate reasoning, 50*(8), 1215-1226.

Labaka, L., Hernantes, J., & Sarriegi, J. M. (2015). Resilience framework for critical infrastructures: An empirical study in a nuclear plant. *Reliability Engineering & System Safety, 141*, 92-105.

Lange, D., Honfi, D., Theocharidou, M., Giannopoulos, G., Kristina, N. K., & Storesund, K. (2017). Incorporation of resilience assessment in critical infrastructure risk assessment frameworks. In M. Cepin & R. Bris (Eds.), *Proceedings of the 27th European Safety and Reliability Conference, ESREL, June 18-22, Portoroz, Slovenia* (pp. 155-163). London, UK: Taylor & Francis Group.

Leach, M. (2008). *Re-framing resilience: Trans-disciplinarity, reflexivity and progressive sustainability–a symposium report* (STEPS Working Paper 13). Brighton: STEPS Centre.

Lee, A. V., Vargo, J., & Seville, E. (2013). Developing a tool to measure and compare organizations' resilience. *Natural Hazards Review, 14*(1), 29-41.

Leitch, M. (2010). ISO 31000: 2009—The new international standard on risk management. *Risk Analysis: An International Journal, 30*(6), 887-892.

Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: Advancing the methodology. *Implementation Science, 5*(1), 69.

Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems, 32*(4), 3317-3318.

Linkov, I., Bridges, T., Creutzig, F., Decker, J., Fox-Lent, C., Kröger, W., . . .Nathwani, J. (2014). Changing the resilience paradigm. *Nature Climate Change, 4*(6), 407.

Liu, W., & Song, Z. (2019). Review of studies on the resilience of urban critical infrastructure networks. *Reliability Engineering & System Safety, 193*, 106617.

Lounis, Z., & McAllister, T. P. (2016). Risk-based decision making for sustainable and resilient infrastructure systems. *Journal of Structural Engineering, 142*(9), F4016005.

Luiijf, E., Nieuwenhuijs, A., Klaver, M., van Eeten, M., & Cruz, E. (2008). Empirical findings on critical infrastructure dependencies in Europe. In R. Setola & S. Gretshuber (Eds.), *Critical Information Infrastructures Security. CRITIS 2008* (pp. 302-310). Berlin, Germany: Springer.

Maclean, K., Cuthill, M., & Ross, H. (2014). Six attributes of social resilience. *Journal of Environmental Planning and Management, 57*(1), 144-156.

Magis, K. (2010). Community resilience: An indicator of social sustainability. *Society and Natural Resources, 23*(5), 401-416.

Manyena, B., O'Brien, G., O'Keefe, P., & Rose, J. (2011). Disaster resilience: a bounce back or bounce forward ability? *Local Environment: The International Journal of Justice and Sustainability, 16*(5), 417-424.

Mayring, P. (2004). Qualitative content analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 1*(2), 159-176.

McDermott, R. (2011). Internal and external validity. In J. N. Druckman, D. P. Green, J. H. Kuklinski, & A. Lupia (Eds.), *Cambridge handbook of experimental political science* (pp. 27-40). Cambridge, UK: Cambridge.

McManus, S. T. (2008). *Organisational resilience in New Zealand*. (Doctoral Thesis), University of Canterbury, New Zealand.

McManus, S. T., Seville, E., Vargo, J., & Brunsdon, D. (2008). Facilitated process for improving organizational resilience. *Natural Hazards Review, 9*(2), 81-90.

Mentzer, J. T., & Flint, D. J. (1997). Validity in logistics research. *Journal of Business Logistics, 18*(1), 199.

Mitchell, E. S. (1986). Multiple triangulation: a methodology for nursing science. *Advances in nursing science, 8*(3), 18-26.

Mostafa, M. A., & El-Gohary, N. M. (2014). Stakeholder-sensitive social welfare–oriented benefit analysis for sustainable infrastructure project development. *Journal of Construction Engineering and Management, 140*(9), 04014038.

Moteff, J. D. (2010). *Critical infrastructures: Background, policy, and implementation* (1437936016). Received through the CRS Web, Order Code RL30153, The Library of Congress.

Munich Re. (2012). *Natural Catastrophes 2011. Analyses, assessments, positions* (Topics Geo). Available from https://www.preventionweb.net/files/25635_30207225en1.pdf.

Naseri, M. (2017). *On Maintainability of Winterised Plants Operating in Arctic Regions.* Paper presented at the ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering.

National Infrastructure Advisory Council (NIAC). (2009). *Critical Infrastructure Resilience: Final Report and Recommendations*. Department of Homeland and Security, U.S. Available from https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf.

National Public Inquiry (NOU). (2006). *Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner* (NOU 2006: 6). Ministry of Justice and Public Security. Oslo, Norway. Available from https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/.

Nemeth, C. P., & Herrera, I. (2015). *Building change: Resilience Engineering after ten years*: Elsevier.

Neuendorf, K. A. (2016). *The content analysis guidebook* (2nd ed.). Los Angeles, USA: Sage.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-based Nursing, 18*(2), 34-35.

Norwegian Directorate for Civil Protection (DSB). (2013). *National Risk Analysis*. Oslo, Norway

Norwegian Directorate for Civil Protection (DSB). (2014). *National Risk Analysis*. Oslo, Norway.

Norwegian Directorate for Civil Protection (DSB). (2017). *Vital functions on society. What functional capabilities must society maintain at all times?* Tønsberg, Norway. Available from https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-ii_english_version.pdf.

Norwegian Police Security Service (PST). (2020). *Nasjonal trusselvurdering 2020*. Oslo, Norway. Available from https://pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-2020-print.pdf.

Onwuegbuzie, A. J. (2000). *Expanding the Framework of Internal and External Validity in Quantitative Research*. Paper presented at the Annual Meeting of the Association for the Advancement of Educational Research (AAER), Ponte Vedra, Florida November 2000.

Organisation for Economic Co-operation and Developmen (OECD). (2014). *Risk Management and Corporate Governance.* (Corporate Governance). Paris, France. Available from http://www.oecd.org/daf/ca/risk-management-corporate-governance.pdf.

Organisation for Economic Co-operation and Development (OECD). (2011). *Future Global Shocks, Improving Risk Governance* (OECD Reviews of Risk Management Policies). OECD Publishing. Available from http://dx.doi.org/10.1787/9789264114586-en.

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability engineering & System safety, 121*, 43-60.

Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability Engineering & System Safety, 141*, 74-82.

Pant, R., Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2014). Stochastic measures of resilience and their application to container terminals. *Computers & Industrial Engineering, 70*, 183-194.

Panteli, M., Trakas, D. N., Mancarella, P., & Hatziargyriou, N. D. (2017). Power systems resilience assessment: Hardening and smart operational enhancement strategies. *Proceedings of the IEEE, 105*(7), 1202-1213.

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis, 33*(3), 356-367.

Paton, D., & Johnston, D. (2001). Disasters and communities: Vulnerability, resilience and preparedness. *Disaster Prevention and Management: An International Journal, 10*(4), 270-277.

Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. *Safety Science, 102*, 79-100.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management Information Systems, 24*(3), 45-77.

Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2017). European Expectations of Disaster Information provided by Critical Infrastructure Operators: Lessons from Portugal, France, Norway and Sweden. *International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 9*(4), 23-48.

Petersen, L., Lange, D., & Theocharidou, M. (2020). Who cares what it means? Practical reasons for using the word resilience with critical infrastructure operators. *Reliability Engineering & System Safety*, 106872.

Petersen, L., Lundin, E., Fallou, L., Sjöström, J., Lange, D., Teixeira, R., & Bonavita, A. (2020). Resilience for whom? The general public's tolerance levels as CI resilience criteria. *International Journal of Critical Infrastructure Protection, 28*(March 2020), 100340.

Petersen, L., Lundin, E., Sjöström, J., Lange, D., & Teixeira, R. (2018). Creating comparable public tolerance and technical performance measures for critical infrastructure resilience evaluation. In S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik, & J. E. Vinnem (Eds.), *Safety and Reliability–Safe Societies in a Changing World: Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway* (pp. 1231-1239). London, UK: Taylor & Francis Group.

Petit, F., Wallace, K., & Philips, J. (2014). *An Approach to Critical Infrastructure Resilience. The CIP Report* Center for Infrastructure Protection and Homeland Security. Volume 12. Number 7.

Pimm, S. L. (1984). The complexity and stability of ecosystems. *Nature, 307*(5949), 321.

Prat, N., Comyn-Wattiau, I., & Akoka, J. (2015). A taxonomy of evaluation methods for information systems artifacts. *Journal of Management Information Systems, 32*(3), 229-267.

Pursiainen, C. (2017). *The Crisis Management Cycle: Theory and Practice*. Oxon, UK: Routledge.

Pursiainen, C. (2018). Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction, 27*, 632-641.

Pursiainen, C., & Gattinesi, P. (2014). Towards testing critical infrastructure resilience. *JRC Scientific and Policy Reports*.

Rerup, C. (2001). "Houston, we have a problem": Anticipation and improvisation as sources of organizational resilience. *Comportamento Organizacional e Gestão, 7*(1), 21-44.

Righi, A. W., Saurin, T. A., & Wachs, P. (2015). A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering & System Safety, 141*, 142-152.

Riolli, L., & Savicki, V. (2003). Information system organizational resilience. *Omega, 31*(3), 227-233.

Robert, B., & Hémond, Y. (2012). Organizational resilience: A multidisciplinary sociotechnical challenge. In *Resilience and urban risk management* (Vol. 119, pp. 119-125): Routledge in association with GSE Research.

Rose, A. (2004). Defining and measuring economic resilience to disasters. *Disaster Prevention and Management: An International Journal, 13*(4), 307-314.

Rose, A., & Krausmann, E. (2013). An economic framework for the development of a resilience index for business recovery. *International Journal of Disaster Risk Reduction, 5*, 73-83.

Rose, A., & Liao, S. Y. (2005). Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions. *Journal of Regional Science, 45*(1), 75-112.

Rosenqvist, H., Reitan, N. K., Petersen, L., & Lange, D. (2018). ISRA: Improver societal resilience analysis for critical infrastructure. In S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik, & J. E. Vinnem (Eds.), *Safety and Reliability–Safe Societies in a Changing World: Proceedings of ESREL 2018, June 17-21, 2018, Trondheim, Norway* (pp. 1211-1220). London, UK: Taylor & Francis Group.

Rossman, G. B., & Rallis, S. F. (2016). *An introduction to qualitative research: Learning in the field*. Thousand Oaks, USA: Sage Publications.

Sapirstein, G. (2006). Social resilience: the forgotten dimension of disaster risk reduction. *Jàmbá: Journal of Disaster Risk Studies, 1*(1), 54-63.

Seel, N. M. (2011). *Encyclopedia of the Sciences of Learning* (Vol. 1). New York, USA: Springer Science & Business Media.

Sherrieb, K., Norris, F. H., & Galea, S. (2010). Measuring capacities for community resilience. *Social Indicators Research, 99*(2), 227-247.

Simmie, J., & Martin, R. (2010). The economic resilience of regions: towards an evolutionary approach. *Cambridge Journal of Regions, Economy and Society, 3*(1), 27-43.

Smith, D., & Fischbacher, M. (2009). The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience. *Risk management, 11*(1), 1-12.

Stephenson, A. V. (2010). *Benchmarking the resilience of organisations.* (Doctoral Thesis), University of Canterbury, New Zealand.

Strunz, S. (2012). Is conceptual vagueness an asset? Arguments from philosophy of science applied to the concept of resilience. *Ecological Economics, 76*, 112-118.

Staat, W. (1993). On abduction, deduction, induction and the categories. *Transactions of the Charles S. Peirce Society, 29*(2), 225-237.

The Council of the European Union. (2008). *On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection* (Council Directive 2008/114/EC of 8 December 2008).

Thomalla, F., Downing, T., Spanger - Siegfried, E., Han, G., & Rockström, J. (2006). Reducing hazard vulnerability: Towards a common approach between disaster risk reduction and climate adaptation. *Disasters, 30*(1), 39-48.

Thornhill, A., Saunders, M., & Lewis, P. (2009). *Research methods for business students*. London, UK: Prentice Hall.

Timmermans, S., & Epstein, S. (2010). A world of standards but not a standard world: Toward a sociology of standards and standardization. *Annual Review of Sociology, 36*, 69-89.

Twigg, J. (2007). *Characteristics of a disaster-resilient community: a guidance note*. Department for International Development (DFID). Available from https://www.preventionweb.net/files/2310_Characteristicsdisasterhighres.pdf.

UNISDR (United Nations Office for Disaster Risk Reduction). (2017). *Words into Action Guidelines. National Disaster Risk Assessment*. Geneva, Switzerland.

United Nations Office for Disaster Risk Reduction (UNISDR). (2009). *Global assessment report on disaster risk reduction* Available from https://www.undrr.org/publication/global-assessment-report-disaster-risk-reduction-2009.

United Nations Office for Disaster Risk Reduction (UNISDR). (n.d.). Terminology on disaster risk reduction Retrieved 28 October 2019 from https://www.unisdr.org/we/inform/terminology

Veenema, T. G., & Woolsey, C. (2003). Essentials of disaster planning. In T. G. Veenema (Ed.), *Disaster nursing and emergency preparedness for chemical, biological, and radiological terrorism and other hazards* (pp. 3-29). New York, USA: Springer Publishing Company.

Verma, T., Araújo, N. A., & Herrmann, H. J. (2014). Revealing the structure of the world airline network. *Scientific Reports, 4*(1), 1-6.

Vickers, M. H., & Kouzmin, A. (2001). 'Resilience' in organizational actors and rearticulating 'voice': Towards a humanistic critique of new public management. *Public Management Review, 3*(1), 95-119.

Vogus, T. J., & Sutcliffe, K. M. (2007). *Organizational resilience: Towards a theory and research agenda.* Paper presented at the 2007 IEEE International Conference on Systems, Man and Cybernetics, Montreal, Canada.

Vugrin, E. D., Warren, D. E., & Ehlen, M. A. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Safety Progress, 30*(3), 280-290.

Walker, B. (1995). Conserving biological diversity through ecosystem resilience. *Conservation Biology, 9*(4), 747-752.

Waller, M. A. (2001). Resilience in ecosystemic context: Evolution of the concept. *American Journal of Orthopsychiatry, 71*(3), 290-297.

White Paper. (2018). *White Paper on Resilience Management Guidelines for Critical Infrastructures. From theory to practice by engaging end-users: concepts, interventions, tools and methods*. Prepared under the Research and Technological Development Crisis Management Topic 7 within European Commission Horizon 2020 Secure Societies Theme. April. Available from http://www.humanist-vce.eu/fileadmin/contributeurs/humanist/white-paper.pdf.

Whittemore, R., Chase, S. K., & Mandle, C. L. (2001). Validity in qualitative research. *Qualitative Health Research, 11*(4), 522-537.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety, 141*, 5-9.

World Economic Forum. (2017). *The Global Risks Report 2017* (Insight Report). Geneva, Switzerland.

Yang, Y., Ng, S. T., Zhou, S., Xu, F. J., & Li, H. (2019). Physics-based resilience assessment of interdependent civil infrastructure systems with condition-varying components: A case with stormwater drainage system and road transport system. *Sustainable Cities and Society*, 101886.

Yin, R. K. (2017). *Case study research and applications: Design and methods*. Thousand Oaks (CA), USA: Sage.

Youn, B. D., Hu, C., & Wang, P. (2011). Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design, 133*(10), 101011.

Yu, C. H. (1994). *Abduction? Deduction? Induction? Is There a Logic of Exploratory Data Analysis?* Paper presented at the Annual Meeting of the American Educational Research Association, New Orleans, USA.

Zhou, H., Wan, J., & Jia, H. (2010). Resilience to natural hazards: A geographic perspective. *Natural Hazards, 53*(1), 21-41.

Part II: Appended papers

Paper I

Characteristics of arctic infrastructure resilience: Application of expert judgement

Rød, B., Barabadi, A., and Gudmestad, O.T. (2016).

Published in *Proceedings of the Twenty-sixth (2016) International Ocean and Polar Engineering Conference* (pp. 1226 – 1233). Rhodes, Greece, June 26-July 1, 2016. ISBN 978-1-880653-88-3; ISSN 1098-6189.

Paper II

Critical Infrastructure Resilience Index

Pursiainen, C., Rød, B., Baker, G., Honfi, D., and Lange, D. (2017).

Published in Walls, Revie & Bedford (Eds.), *Risk, Reliability and Safety: Innovating Theory and Practice. Proceedings of the 26th European Safety and Reliability conference, ESREL* (pp. 2183 – 2189). Glasgow, Scotland, September 25-19, 2016. London, UK: Taylor & Francis Group. ISBN 978-1-138-02997-2.

Risk, Reliability and Safety: Innovating Theory and Practice – Walls, Revie & Bedford (Eds)

Critical infrastructure resilience index

C. Pursiainen & B. Rød
The Arctic University of Norway, UiT, Norway

G. Baker
SP Fire Research AS, Norway

D. Honfi & D. Lange
SP Technical Research Institute, Sweden

ABSTRACT: The article presents a holistic, easy-to-use and computable methodology to evaluate critical infrastructure resilience, called Critical Infrastructure Resilience Index. The methodology is applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors and facilities as well as hazard scenarios. The aim, and the innovative potential, is to be able to transfer the quantitative, semi-quantitative and qualitative evaluations of individual sector-specific resilience indicators into uniform metrics, based on process maturity levels. In this article, we first concisely present the methodology. Second, we illustrate how this methodology could be applied to a specific infrastructure and hazard scenario.

1 INTRODUCTION

In the recent years, the focus has moved from critical infrastructure protection to that of resilience. But how do we know whether a critical infrastructure is resilient or not, how can it be evaluated, measured and enhanced?

Drawing on, combining and developing the ideas of the existing literature and practices, briefly referred to here, the article develops a holistic, easy-to-use and computable methodology to evaluate critical infrastructure resilience, called Critical Infrastructure Resilience Index (CIRI). The methodology is applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors, facilities and hazard scenarios. The proposed methodology is especially suitable for organizational and technological resilience evaluation.

The methodology developed here makes it possible to come up with a single quantitative value for the selected critical infrastructure's overall resilience. However, one can also choose to focus on resilience of only part of the infrastructure, or only some selected indicators, or resilience related to a specific hazard scenario. In the latter cases, the aggregated value then represents only the chosen focus.

The user of this methodology is supposed to be the operator of critical infrastructure in the spirit of self-auditing. In case it would be implemented in a wider scale and monitored by the authorities, it would give them a holistic picture about the respective society's critical infrastructure resilience.

2 GENERAL METHODOLOGY

2.1 *Definition of resilience*

The European Union Directive from 2008 (European Council, 2008) defines critical infrastructure as follows: "An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." The Directive focuses on critical infrastructure protection, which it defines as "all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability."

While there are several definitions of the concept of resilience, a suitable generic definition for our purposes is provided by UNISDR (2009): "The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions."

It is notable that the verb 'resist' implies that protective measures are included. Resilience can thus be understood as an umbrella concept covering also critical infrastructure protection. In our scheme, it then basically covers all the 'phases' of the traditional crisis management cycle, to be discussed below.

2.2 *Resilience domains*

The exact boundaries of the resilience discourse in the context of critical infrastructure are still rather obscure. Nevertheless, certain sub-discourses have emerged, and even become institutionalized. Consequently, we can differentiate between at least three separate, though partially overlapping, domains of (critical infrastructure) resilience: *societal* (e.g. Sherrieb et al., 2010; McAslan, 2010a; Cutter et al., 2008; Norris et al., 2008; Klein et al., 2003; Bruneau et al., 2003); *organisational* (e.g. Labaka et al., 2015; Prior, 2015; Petit et al., 2014; Petit et al., 2013; Linkov et al., 2013; McAslan, 2010b; ISO, 2011; cf. ISO, 2007; ISO, 2014a-c); and *technological* (e.g. Labaka et al., 2015; Prior, 2015; Petit et al., 2014; Petit et al., 2013; Linkov et al., 2013; McAslan, 2010b). We call these dimensions *resilience domains*. When defining the resilience domain, we in principle can approach the question *who* or *which* organisations or institutions are in charge in measuring a certain critical infrastructure resilience indicator and taking the appropriate actions after the fact that a measurement has pointed out a potential problem or gap. In societal resilience, the important actors are national and local governments, communities and households. In organizational resilience, the actors are the businesses, especially those responsible for critical infrastructures and supply chains. In technological resilience, the actors are critical infrastructure operators and, to some extent, safety and security manufacturers and vendors.

While the societal resilience concept is important, it is not very helpful from the critical infrastructure operators' point of view as it is mostly beyond their influence. Therefore, we here focus on organisational and technological resilience that are the domains most closely related to critical infrastructure resilience.

2.3 *The temporal dimension of resilience*

The above UNISDR resilience definition implies that there is a certain temporal dimension of resilience. Resilience is thus a process that has to be present and enhanced before, during and after the disruption of critical infrastructure service. Connecting the measurement and enhancement strategy to the temporal dimension of resilience helps to identify both *when* and *what* should be done in order to enhance resilience.

A typical way to express this temporal dimensions is the performance loss triangle (Chang et al., 2014; Bruneau et al., 2003; McDaniels et al., 2007), which presupposed the mode of operation before, during and after the stress against a critical infrastructure. Thus, in the approach developed by the U.S. Department of Homeland Security (HSSAI, 2009; cf. Nieuwenhuijs et al., 2008) it is differentiated between three resilience objectives that are interrelated and reinforcing; namely resistance, absorption, and restoration, resistance being the operational mode before and after the disruption.

Another way to take into account the temporal dimension, which we follow here, is to understand

Figure 1. The Crisis Management Cycle.

resilience in the context of the crisis management cycle (e.g. Kozine & Andersen, 2015; Petit et al., 2014; Petit et al., 2013). In its standard version, this cycle includes at least pre-, during and post-crisis phases, often further divided into subject areas or phases, which are sequential. For resilience measurement purposes, it is useful to have rather more than less phases, as this zooms our focus in on less abstract and more singled out - and therefore more measurable - indicators. In this article, we therefore distinguish between the following phases/subject areas: 'Risk assessment'; 'Prevention' (including pre-event mitigation); 'Preparedness'; 'Warning' (including monitoring and early warning); 'Response' (including post-event mitigation/damage limitation and consequence management); 'Recovery' (including restoration and reconstruction); and 'Learning' (including post-crisis evaluation). These phases are illustrated in Figure 1; later in the article, they represent what we call Level 1 indicators.

For most of these crisis management phases, rather clear-cut and generally accepted definitions can be found (e.g. UNISDR, 2009). While 'Learning' is not included, in the strict meaning, in the above referred UNISDR resilience definition, it has become more and more understood both in literature and practice that learning during and from incidents, emergencies and disasters is one of the key issues in crisis management (Drupsteen & Guldenmund, 2014; Müller-Seitz, 2014). We therefore add also this element into our model.

2.4 *The overall scheme*

Based on the resilience domains and the crisis management cycle, the task is to develop a set of indicators to measure critical infrastructure resilience, thus making it possible to identify and plan the respective measures to enhance resilience. An indicator is a sign that shows the condition or existence of something, and it is typically understood as a measurable variable used as a representation of an associated factor or quantity. When put together, we call the collection of indicators a Critical Infrastructure Resilience Index (CIRI).

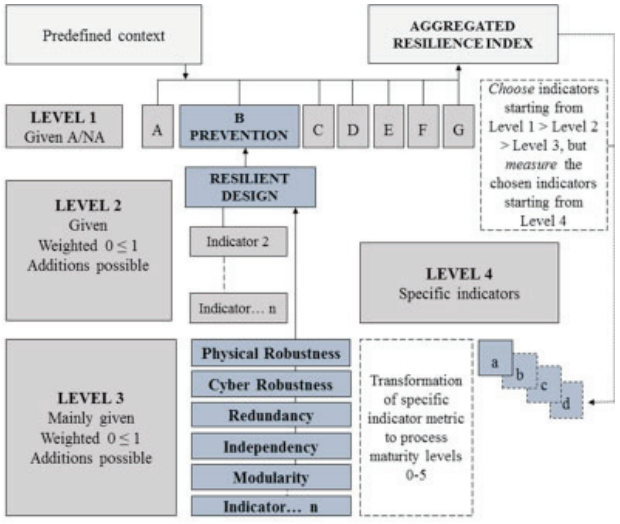

Figure 2. CIRI overall scheme.

The overall scheme of CIRI is presented in Figure 2, with some indicators illustratively presented under 'Prevention' as a hierarchic path.

Related to the *metrics* that is used in CIRI, to be discussed below, we define indicators, be they originally representing any type of qualitative, semi-quantitative or quantitative metrics, transferrable into processes, procedures, series of actions and operations, schemes, methods, systems, or quality and quantity that enable a certain condition or performance.

2.5 *Establishing the context*

Like in risk assessment, the process of measuring resilience starts with establishing the context. This includes defining three sets of variables: the domain, the hazard type, and situational factors. There is therefore a considerable freedom to tailor the focus of the particular context one is interested in.

The domain

While to somewhat overlapping, each resilience domain has its own sets of indicators, or the same indicator is defined differently. In our methodology, one can choose both organizational and technological domain, or only one of them.

Choosing the domain(s) serves two purposes. First, it tells us what kind of indicators we are supposed to measure. Second, it tells us about the meaning of our results. We may aggregate a certain resilience value with our methodology, described below, and knowing the domain, we can present the outcome as reflecting the resilience domain(s) in question and not something else.

The hazard type

Each hazard type may demand different types of resilience measures, which means that resilience is potentially also measured through different indicators depending on the hazard. A critical infrastructure may be maximally resilient against natural hazards but very vulnerable against malicious attacks. In the former case, physical access control, for instance, does not play a significant role, whereas in the latter case it is crucial.

Following the EU risk evaluation summary (European Commission, 2014), we differentiate between natural, non-malicious man-made, malicious man-made, and multi-hazards. The methodology allows to choose all of them or concentrating only on resilience in the context of a certain type of hazard.

Situational factors

Resilience depends also on situational factors. Loosing electricity, for instance, is quite a different thing in summer time during working hours or in cold and stormy winter conditions during banking holidays with minimum staff available for unplanned maintenance and recovery. This set of variables is tailorable (one can choose/add location, weather conditions, seasonality, etc.) or its pre-defined elements can be marked as NA (not applicable).

In other words, one can concretize the measurement of indicators with a suitable hazard scenario. Scenario building is specifically a method to examine complex developments. Like in risk assessment, it is usually only in scenarios one may combine many risk factors in ways to create some surprising events that are difficult to formalize, but which however simulate better the characteristics of a real-life disaster.

2.6 *Levels*

In order to operationalise the methodology, we have chosen to differentiate between four hierarchic levels of indicators. While *choosing* the indicator that one wants to measure, one should start from Level 1 downwards. However, the very *measurement* takes place on Level 4, and the other levels' values are derived from these measurements. So Levels 1–3 are aggregations of Level 4 indicators, rather than genuine measurable indicators as such. For the sake of simplicity of language, we however call these aggregated variables as indicators below.

Level 1: The crisis management cycle phases

Level 1 consists of set of (aggregations of) indicators that are the very same crisis management cycle phases already presented above in Figure 1. In Figure 2, these phases are represented with symbols A-G. This level is a generic one and applicable to all types of critical infrastructure. They are not subjects to change but given in our methodology, and it is assumed that each Level 1 indicator (cycle phase) is equally important. However, if needed, one can choose one or several of them as 'not applicable' (NA), that is, one chooses for the time being to focus only on a certain phase or phases for the sake of lack of time or specific needs of analysis. This might also be the case if, for instance, one has not the data available to consider a certain phase. This refers especially to 'Response' and 'Recovery' phases. That is so, because we define them to

be measurable (that is, applicable) only on the basis of historical event data in order to avoid measuring indicators twice, as many preparedness measures are actually about preparing to response or recovery.

Level 2: The generic indicators
Level 2 represents such set of (aggregations of) indicators that are generic applications of Level 1. The methodology permits to choose any of Level 2 predetermined indicators as not applicable (NA). If so, they will not be taken into account when calculating the total resilience value. The methodology also allows adding some new Level 2 indicators, depending on the operator's needs. While the assumption is that the chosen Level 2 indicators are equally important, a possibility of weighing (NA$\leq$1) is included.

Combining Levels 1 and 2 into a same matrix, a simple framework for a resilience index emerges, as presented in the table in *Appendix 1*. The uppermost row represent the Level 1 (the crisis management cycle phases), the rest provide a kind of a blueprint of possible Level 2 indicators, to be tailored by weighing and adding new indicators by the operator.

We have not populated totally the matrix on Level 2, but rather provide a blueprint of the most generic groups of organisational and technological indicators that are usually discussed in resilience literature (with somewhat varying vocabulary). Such an indicator would be, for instance, 'Resilient design', which is located under Level 1 'Prevention'.

Note that both organisational and technological indicators can be approached by this blueprint, as Level 2 indicators often, but not always, can be applied to both domains. 'Resilient design', for instance, may refer to the design of system redundancy, which further can be measured by organisational indicators, such as the existence of alternative site for critical operations, or technological indicators, such as the existence of reserve power source. The selected domain(s) then define which indicators one should be focusing on.

Level 3: Dividing the generic indicators into parts
Level 3 represents such set of (aggregations of) indicators, which is a typological application of Level 2; that is, it divides Level 2 indicators into smaller and more easily measurable processes or systems. For instance, should we have chosen 'Resilient design' as Level 2 indicator, for a technological system on Level 3 this might mean that we focus on such indicators under this general theme as 'Physical Robustness', 'Cyber Robustness', 'Redundancy', 'Modularity', 'Independency. This is illustrated in Figure 2 above.

While also these types of indicators are rather generic, we allow that some of them might be not applicable (NA) for some sectors, some facilities or some hazard scenarios, or they might be of lesser value compared to indicators that are more important. Thus the possibility of weighing (NA$\leq$1) applies also here. Similarly as on Level 2, some tailored indicators can be added by the operator.

Level 4: Indicators to be measured
Given that an operator has decided upon the above Levels 1-3 and respective sets of (aggregations of) rather generic indicators that one is interested in, one has to specify or tailor the indicators at Level 4 according to one's sector (e.g. health care, electricity grid, rescue services, bridges). Preferably, one should also focus on a certain facility or function within the sector in focus (e.g. a hospital, energy production and distribution in a certain city, municipal tap water distribution, local rescue service, a certain bridge or a tunnel).

In practice, resilience indicators at this level have to be detailed carefully according to the characteristics of the concrete facility. Level 4 is therefore to specify the indicator depending on the concrete application. One should notice that on Level 4 there might be several indicators under one of the Level 3 indicators, that is, 4a, 4b, 4c, and so forth. These indicators are always specific and measured by their own metrics. This might include any quantitative, semi-quantitative or qualitative processes.

The measurement of these indicators however might be, and often are, an already fully existing practice in a critical infrastructure facility, and the information would then be readily available. In this case, the current CIRI methodology helps to systematize the measurements. Sometimes the current methodology might guide to investigate a completely neglected indicator, and therefore a new measurement methodology might be needed.

2.7 *Maturity metrics*

After measuring the selected Level 4 indicators, one should go upwards again. The challenge then is to transform these Level 4 measurements into the commensurable metrics on Level 3 values. For this task, we rely on the COBIT (4.1) general maturity model consisting of six maturity levels, as indicated in Table 1. (For more detailed explanation, see COBIT 2007, pp. 18, 19; for COBIT 5, cf. COBIT 2012.)

The above standard table might be enough to consider a certain Level 4 indicator's value to be transformed on the scale 0–5. However, we expect that in many cases it is useful to tailor the scale descriptions, using a regulation, existing standard, best practice, experience, or expert opinions. Hospital building codes, for instance, include regulations about the minimum requirements for reserve power source, which could guide the definitions of the scaling descriptions in that indicator. This does mean that the operator, who is doing the resilience measurement, has always to carefully consider each indicator and its resilience value in comparative perspective. Should we measure quantity, for instance, as we do in our illustrative case below, what becomes important is to tailor the quantity scale onto the scale between nonexistent (0) and optimized (5) based on some justified ground.

Table 1. COBIT maturity levels.

Level 3		Level 4
0	**Non-existent**	Specific metrics of any indicator is transformed into processes, procedures, series operations, schemes, methods or systems, corresponding one of the maturity levels 0–5.
1	(Initial/Ad hoc)	
2	(Repeatable but Intuitive)	
3	(Defined Process)	
4	(Managed and Measurable)	
5	**Optimised**	

2.8 *Calculating the overall resilience*

The overall CIRI is calculated based on the above four levels of indicators, by simple aggregation. Let us assume that we have done our measurements on Level 4. Then we start by aggregating all the Level 4 information to get a score for all the Level 3 indicators, following the maturity scale presented in Table 1. Note that one might want to weigh the data to get the correct picture, depending on the operator's subjective evaluation. Mathematically we end up with the following algorithm, to calculate the resilience index, starting from Level 3, calculating the individual Level 2 indicators:

$$Level\ 2 indicator = \frac{1}{\sum_{i=1}^{m} w_i} \sum_{i=1}^{m} w_i\, L3 indicator_i \qquad (1)$$

Here m is the number of Level 3 indicators, and w_i represents the weighting coefficients for the individual Level 3 indicators with a value between 0 and 1 corresponding to the indicators' relevance. Further, the seven Level 1 indicators are estimated as follows:

$$Level\ 1 indicator = \frac{1}{\sum_{i=1}^{n} v_i} \sum_{i=1}^{n} v_i\, L2 indicator_i \qquad (2)$$

Here n is the number of Level 2 indicators and $v_i$the weighting coefficients for the individual Level 2 indicators. To produce the final resilience index, the seven Level 1 indicators are consequently aggregated into one score (representing the chosen context and focus):

$$CIRI = \frac{1}{7} \sum_{i=1}^{7} L1\ indicator_i \qquad (3)$$

The result of an imagined measurement is presented in Figure 3.

3 HOW TO USE THE METHODOLOGY

The index makes full sense only if several indicators are analyzed and the accumulated resilience value calculated. In the following, however, we illustrate how Level 4 indicator can be defined under a certain scenario, and especially how it is transformed into a Level 3 indicator.

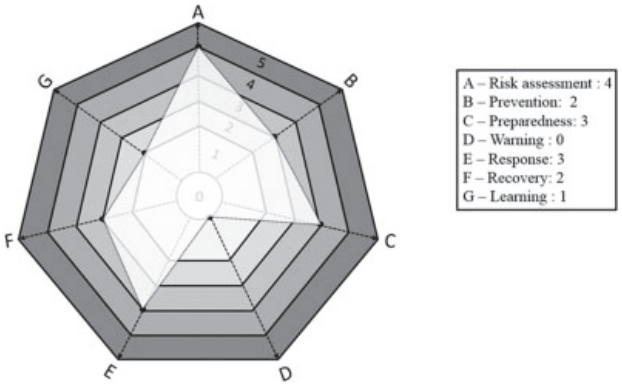

Figure 3. CIRI radar.

3.1 *Context: The scenario*

Let us imagine the following context:

Domain: Technological
Hazard Type: Man-Made Non-Malicious
Situational Factors: Scenario on disruption of aviation fuel transport to Oslo Airport Gardermoen

Oslo Airport Gardermoen is the largest airport in Norway and one of three regional hubs for SAS Scandinavian Airlines. All the aviation fuel for Oslo Airport Gardermoen comes from Sydhavna, Oslo. Aviation fuel is stored in an underground cistern at Ekeberg Oil Storage, which is part of the Ekebergåsen Fuel Depot facility at Sydhavna.

A man-made non-malicious incident, i.e., an accident of some kind, has occurred at Sydhavna which prevents aviation fuel being supplied from the Ekebergåsen Fuel Depot facility to Oslo Airport Gardermoen for 3 months. While concerning this scenario, and omitting other situational factors, the objective of this example is to measure the indicator Level 1: Prevention > Level 2: Resilient Design > Level 3: Redundancy, in terms of reserve fuel capacity. For that, we will develop a quantifiable Redundancy Metric that can be linked to the length of time of disruption to service, further to be called the Impact Metric, in this case the supply of aviation fuel from Sydhavna to Oslo Airport Gardermoen.

3.2 *Level 4 indicators: Reserve storage capacity*

Oslo Airport Gardermoen is supplied with aviation fuel from the depot in Ekebergåsen by rail using specially adapted wagons. At the level of activity at Oslo Airport Gardermoen in 2012 of 20 million passengers, 9 train loads of fuel were required per week, with each train carrying approximately 1150 m^3 of product. Over the three month (13 week) period of disruption to aviation fuel supplies from Sydhavna, based on the 2012 consumption figures, a total of 117 train loads of fuel would be required to maintain normal levels of flight/passenger activity at the airport. This equates to a total volume of 134550 m^3 of aviation fuel.

Oslo Airport Gardermoen does have a small capacity of on-site storage (2–4 days). For the purpose of the analysis there is therefore assumed to be 4 train loads of fuel stored at the airport when the incident

Table 2. Impact Metric and Redundancy Metric.

	Impact Metric	Redundancy Metric
0	Service disrupted for more than 90 days	0 m^3 reserve storage capacity
1	Service disrupted for 30–90 days	38630 to 4 600 m^3 reserve storage capacity
2	Service disrupted for 7–30 days	53440 to 38 630 m^3 reserve storage capacity
3	Service disrupted for 3–7 days	56020 to 53 440 m^3 reserve storage capacity
4	Service disrupted for less than 3 days	57950 to 56 020 m^3 reserve storage capacity
5	No disruption to service	57950 m^3 reserve storage capacity

occurs, or 4600 m^3 of fuel. This reduces the required volume of fuel, during the 90 day period of disruption, to 129950 m^3. The only alternative way to transport aviation fuel to Oslo Airport Gardermoen is via tank-trucks. At a capacity of 40 m^3 per tank-truck, 30 tank-truck loads are required to match the capacity of one train load. The greatest practical problem will be the availability of tank-trucks that can transport aviation fuel.

For the purpose of this analysis, it is assumed that an average of 20 tank-truck deliveries per day, throughout the 3 month period of disruption, are able to be arranged as an alternative to the rail supply system from Sydhavna. During the 90 day period of the disruption, this amounts to 72000 m^3 of aviation fuel, reducing the total amount of fuel storage required to avoid any disruption to airport services to 129500–72000 = 57950 m^3. At a daily consumption rate of approximately 1440m^3 per day of normal operation, this equates to 40 days' supply of aviation fuel.

The Impact Metric chosen for this example is length of time of disruption of service, with the range of possibilities tailored to suit the specifics of the incident scenario, i.e., 0 to 90 days. In Table 2, Column 'Impact Metric', the 0 to 5 range of our maturity model is arbitrarily applied to the duration of the period of disruption to service that is applicable to this incident scenario. Having quantified the Impact Metric, the chosen mitigation strategy, in addition to the ability to receive 20 tank-truck loads of aviation fuel per day, is to invest in reserve storage capacity of 57950 m^3, in addition to the 4600 m^3 that already exists at Oslo Airport Gardermoen. This is expressed in Table 2, Column 'Redundancy Metric'. The Redundancy Metric is therefore a volume of reserve storage capacity, where 57950 m^3 equates to no disruption to service, based on the analysis presented above, and the existing storage capacity of 4600 m^3 equates to slightly less than 90 days' disruption. To calculate the resilience indicator on scale 0–5 in our case therefore presupposes to check the reserve storage capacity, as in Table 2.

4 CONCLUSIONS

We have above presented the Critical Infrastructure Resilience Index (CIRI) and demonstrated its methodology. The methodology is applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors, facilities and hazard scenarios. The proposed methodology is suitable especially for organisational and technological resilience evaluation. The innovative potential is that with CIRI one is able to transfer the quantitative and qualitative evaluations of individual sector-specific resilience indicators into uniform metrics, based on process maturity levels. Its main usefulness is that it enables to measure several indicators and transform them into one metrics, and thus making it possible to define the aggregated level of resilience on the scale 0-5. The methodology is also suitable to be developed into a software-based application.

ACKNOWLEDGMENTS

The article is a by-product of the IMPROVER project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 653390.

REFERENCES

Bearse, R. 2014. The Return on Investing in Personal resilience. *The CIP Report*, Center for Infrastructure Protection and Homeland Security, Volume 12 Number 7, January 2014, pp. 21–24.

Boone, W. 2014. Functional Resilience: The 'Business End' of Organizational Resilience, *The CIP Report*, Center for Infrastructure Protection and Homeland Security, Volume 12 Number 7, January 2014, pp. 5–8.

Bruneau, M. et al. 2003. A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectre*, 2003 19(4), pp. 733–752.

Chan, S.L. et al. 2014. Establishing Disaster Resilience Indicators for Tan-sui. *Soc Indic Res,* Volume 115, pp. 387–418.

Cutter, S.L. et al. 2008. A place-based model for understanding community resilience to natural disasters. *Global Environmental Change* 18(2008), pp. 598–606.

COBIT 2007. *Cobit 4.1 Excerpt. Executive Summary Framework*. United States of America: IT Governance Institute. [Online] Available from: https://www.isaca.org/KnowledgeCenter/cobit/Documents/COBIT4.pdf

Drupsteen L. & Guldenmund, F.W. 2014. What Is Learning? A Review of the Safety Literature to Define Learning from Incidents, Accidents and Disasters. *Journal of Contingencies and Crisis Management*, Volume 22, Number 2, June, pp. 81–96.

European Commission 2014. *Overview of natural and man-made disaster risks in the EU.* Commission Staff Working Document. Brussels, 8.4.2014. SWD(2014) 134 final.

European council 2008. *On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* Council Directive 2008/114/EC of 8 December 2008.

Francis, R. & Bekera, B. 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering and System Safety* 121 (2014), pp. 90–103.

HSSAI 2009. *Concept Development: An Operational Framework for Resilience*. Homeland Security Studies and Analysis Institute. August 27, 2009.

ISO 2007. Security management systems for the supply chain. International Standardization Organization. Guidelines for the implementation of ISO 28000. 28004:2007.

ISO 2011. *Security management systems for the supply chain – Development of resilience in the supply chain*. International Standardization Organization. 28002:2011.

ISO 2014a. *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations*. International Standardization Organization. 28004-2:2014.

ISO 2014b. *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 3: Additional specific guidelines for adopting ISO 28000 for use of medium and small businesses (other than marine ports).* International Standardization Organization. 28004-3:2014.

ISO 2014c. *Security management systems for the supply chain. Guidelines for the implementation of ISO 28000. Part 4: Additional specific guidelines for adopting ISO 28000 if compliance with ISO 280001 is a management objective.* International Standardization Organization. 28004-4:2014.

ISO/IEC 2009. *Risk management – Risk assessment techniques.* International Standardization Organization. IEC/FDIS 31010.

ISO/PAS 2007. *Societal security - Guideline for incident preparedness and operational continuity management.* International Standardization Organization. ISO/PAS 22399:2007.

Klein, R.J.T., Nicholls, R.J. & Thomall F. 2003. Resilience to natural hazards: How useful is this concept? *Environmental Hazards* 5 (2003), pp. 35–45.

Kozine I., & Andersen, H.B. 2015. Integration of resilience capabilities for Critical Infrastructures into the Emergency Management set-up. In. Podofillini et al. (Eds), *Safety and Reliability of Complex Engineered Systems*. London: Taylor & Francis Group, London, pp. 172–176.

Labaka, L., Hernantes, J. & Sarriegi, J.M. 2015. Resilience framework for Critical Infrastructures: An Empirical Study in a Nuclear Plant, *Reliability Engineering and System Safety* 141, pp. 92–105.

Linkov, I. et al. 2013. Measurable Resilience for Actionable Policy. *Environmental Science and Technology*, 47, pp. 10108–10110.

McAslan, A. 2010a. *Community Resilience. Understanding the Concept and its Applications*. [Online] Available from: http://sustainablecommunitiessa.files.wordpress.com/2011/06/community-resilience-from-torrens-institute.pdf

McAslan, A. 2010b. *Organisational Resilience. Understanding the Concept and its Application*. [Online] Available from: http://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0CDoQFjAC&url=http%3A%2F%2Fwww.executiveaccelerators.com.au%2FLiteratureRetrieve.aspx%3FID%3D129836&ei=zSbVUv66GIinyQOGn4GICg&usg=AFQjCNHvoywQ-bRpx9FZRc5yw6t7oQh5w&bvm=bv.59378465,d.bGQ

Mcdaniels, T. et al. 2007. Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems*, 13(3), pp. 175–184.

Müller-Seitz, G. 2014. Learning during crisis as a 'war for meaning': The case of the German Escherichia coli outbreak in 2011. Management Learning 2014, Vol. 45(5), pp. 593–608.

Nieuwenhuijs, A.H., Luiijf, H.A.M. & Klaver, M.H.A. 2008. Modeling Critical Infrastructure Dependencies. In MAURICIO, P. and SHENOI, S. (eds.). *IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II*, Boston: Springer, October 2008, pp. 205–214.

Norris, F.H. 2008. Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology*, 41, pp. 127–150.

Petit, F.D. et al. 2013. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Argonne National Laboratory, U.S. Department of Energy, April.

Petit, F., Wallace, K. & Phillips, J. 2014. An Approach to Critical Infrastructure Resilience. *The CIP Report*, Center for Infrastructure Protection and Homeland Security. Volume 12 Number 7, January, pp. 17–20.

Prior, T. (2015) *Measuring Critical Infrastructure Resilience: Possible Indicators.* Risk and Resilience Report 9. ETH Zürich: April. Rodriguez-Llanes, J.M., Vos, F. & Guha-Sapir, D. 2013. Measuring psychological resilience to disasters: are evidence-based indicators an achievable goal? *Environmental Health*, 12:115, pp. 1–10.

Rose, A.Z. 2009. *Economic Resilience to Disasters*, CARRI Research Report 8, CREATE Research Archive, Published Articles & Papers, 11-1-2009, pp. 7–8.

Rose, A. & Krausman, E. 2013. An Economic Framework for the Development of a Resilience Index for Business Recovery. *International Journal of Disaster Risk Reduction* 5, pp. 73–83.

Sherrieb, K., Norris, F.H. & Galea, S. 2010. 'Measuring Capacities for Community Resilience', *Soc Indic Res* 99, pp. 227–247.

UNISDR 2009. *UNISDR Terminology on Disaster Risk Reduction*, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009. [Online] Available from: http://www.unisdr.org/we/inform/terminology

Appendix 1: Levels 1 and 2.

Risk assessment	**Prevention**	**Preparedness**	**Warning**	**Response**	**Recovery**	**Learning**
Failure data gathering	Safety and security culture	Preparedness plan and crisis organization	Audits	Situation awareness	Downtime	Evaluation
Knowledge of the context	Physical and cyber entrance control	Redundancy plan	Monitoring	Decision-making	Reduced service level	Institutional Learning
Risk assessment procedure	Risk treatment plan	Cooperation agreements (external resources)	Early warning and alarm	Coordination (internal and external)	Costs	Implementation of lessons
Monitoring and review	Risk communication	Capability building		Communication (internal and external)	Unplanned maintenance	Technological upgrading
Testing and simulation	Resilience plan	Capacity building		Resource deployment	Restart	
	Resilient design	Technical supportability		Absorption/ damage limitation	Autonomy	
	Planned maintenance	Interoperability (internal and external)		Externalised redundancy	Insurance	
	Information sharing	Stakeholder management				

Paper III

Evaluation of resilience assessment methodologies

Rød, B., Pursiainen, C., Reitan, N.K., Storesund, K., Lange, D., and Mira da Silva, M. (2018).

Published In M. Cepin & R. Bris (Eds.), *Safety and Reliability – Theory and Applications. Proceedings of the 27th European Safety and Reliability Conference, ESREL* (pp. 1039 - 1051). June 18-22, 2017, Portoroz, Slovenia. London, UK: Taylor & Francis Group. ISBN 978-1138629370.

Safety and Reliability – Theory and Applications – Čepin & Briš (Eds)

Evaluation of resilience assessment methodologies

B. Rød & C. Pursiainen
UiT The Arctic University of Norway, Tromso, Norway

N. Reitan & K. Storesund
SP Fire Research AS, Norway

D. Lange
SP Technical Research Institute of Sweden, Sweden

M. Mira da Silva
INOV INESC Inovação, Lisboa, Portugal

ABSTRACT: There are a wide range of different frameworks and methodologies for analysing Critical Infrastructure (CI) resilience, covering organisational, technological and social resilience. However, there is a lack of a clear methodology combining these three resilience domains into one framework. The final goal of the ongoing EU-project IMPROVER, 'Improved risk evaluation and implementation of resilience concepts to Critical Infrastructure,' is to develop one single improved and easy-to-use critical infrastructure resilience analysis tool which will be applicable within all resilience domains and to all types of critical infrastructure. This article presents part of this work, in which IMPROVER comprehensively evaluated, by demonstration and comparison, a selection of existing resilience methodologies in order to integrate their best features into the new methodology. The selected methodologies were The Benchmark Resilience Tool (BRT) (Lee et al., 2013), Guidelines for Critical Infrastructures Resilience Evaluation (CIRE) (Bertocchi et al., 2016) and the Critical Infrastructure Resilience Index (CIRI). The latter was developed within the consortium (Pursiainen et al., 2017). The results show that it is hard to evaluate and compare the different methodologies considering that the methodologies are not aiming to achieve the same thing. However, this evaluation shows that all the methodologies have pros and cons, and that the IMPROVER project should aim at combining, in so far as is possible and commensurable, the identified pros while avoiding the identified cons into a Critical Infrastructure resilience assessment framework compatible with the current guidelines for risk assessment in the Member States.

1 INTRODUCTION

Due to recent disruptive events there has been a shift from protection to resilience of critical infrastructure (Pursiainen et al., 2017). This has led to the development of new methodologies to assess Critical Infrastructure (CI) resilience, which not only concentrate on protection, but also on capabilities such as response and recovery. Resilience indicators, characterised as qualitative and/or quantitative, are used within most of the resilience assessment methodologies and represent measureable indicators that constitute parts of the overall critical infrastructure resilience – such as robustness, redundancy, resilient design and so on. The questions are how the resilience concepts should be selected, how they should be measured and how they contribute to the overall resilience of critical infrastructure.

This work aims to evaluate the contribution of individual resilience indicators to the resilience of critical infrastructure and to evaluate a number of existing methodologies for implementation of resilience indicators to critical infrastructures. In section 2 of this paper, the concepts of critical infrastructure resilience and resilience assessment are briefly described. In section 3, the three selected methodologies are briefly presented. In section 4, a set of individual indicators are selected as 'test' indicators for a discussion of their relevance to the three selected methodologies. Additionally, two fictional scenarios/living labs, representing different critical infrastructures, are described. In section 4, the use of methodologies against the scenarios is demonstrated with the selected indicators. Finally, in section 5, the three methodologies are evaluated and their performances compared, identifying their pros and cons based on the author's experiences from using the methodologies for the illustration and the demonstration.

2 DEFINITION OF CRITICAL INFRASTRUCTURE RESILIENCE ASSESSMENT

There exists a wide range of different definitions of *resilience* from different domains, but to date, there exists no standardised definition of resilience. However, in the IMPROVER project there is a common agreement that the definition from the United Nations International Strategy for Disaster Reduction (UNISDR, 2009) provides a suitable generic definition of resilience as 'the ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions.' From this definition, it is clear that resilience can be understood as an umbrella concept, including several capabilities and features, such as protection, resistance, absorption, accommodation, responsiveness and recoverability, covering both pre- and post-event activities.

While there are many different definitions of resilience, there is a higher degree of consensus within the field of civil protection on the definition of *critical infrastructure*. The European Union Directive 2008/114/EC – identification and designation of European critical infrastructures and assessment of the need to improve their protection – defines critical infrastructure as follows: 'An asset, system or part thereof located in Member States which is essential for maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.'

In the context of critical infrastructure, resilience can be defined within different *resilience domains*. However, to draw exact borders between the domains can be a difficult, if not impossible, task. Nevertheless, a few domains have emerged, and in this work, we differentiate between societal, organisational and technological resilience. Even though these domains are separated, it should be noted that there is obviously a high degree of overlap between them.

2.1 *Resilience assessment*

The IMPROVER consortium proposes the following definitions for the various stages of a resilience assessment framework based on the equivalent ISO 31000 definitions for risk assessment:

- **Resilience analysis** is the process of comprehending and determining the level of resilience based on selected resilience indicators.
- **Resilience evaluation** is the process of comparing the results of resilience analysis with criteria or objectives to determine whether the resilience level is acceptable and to identify areas for improvement.
- **Resilience assessment** is the overall process of resilience analysis and evaluation.

3 EXISTING RESILIENCE ASSESMENT METHODOLOGIES

There exist several methodologies to study critical infrastructure resilience. However, there are large deviations between the background, focus and application of the individual methodologies. A few of the methodologies are in operational use, while most of them only exist as theoretical and methodological models. In the current context, based on previous work in IMPROVER, the following seven methodologies for analysing resilience have been longlisted and considered relevant for the study of critical infrastructure resilience:

- Critical Infrastructure Resilience Index (CIRI) (Pursiainen et al., 2017).
- Resilience Management Index (Lee et al., 2013)
- Benchmark Resilience Tool (BRT) (Petit et al., 2013).
- Guidelines for Critical Infrastructure Resilience Evaluation (CIRE) (Bertocchi et al., 2016).
- Organisational Resilience Health Check (Australian Government, http://www.organisationalreince.gov.au/HealthCheck/Pages/default.aspx [Accessed: 14 November 2016].
- Resilience Analysis Grid (Hollnagel, 2015).
- Measuring Resilience: Benefits and Limitations of Resilience Indices (Prior, 2015).

The majority of the available methodologies for studying resilience are methodologies for resilience analysis, according to the definition in section 2.1. The subsequent stage of resilience evaluation is often missing, and where it is present, it exists only in the form of limited comparisons of the resilience of the organisation, asset or system in question with other comparable objects. The weakness with implementation of resilience concepts to critical infrastructure on this basis is that it risks being arbitrary with a narrow focus. Therefore, there is a need for a framework for resilience assessment which includes a thorough evaluation process based on the needs and requirements from stakeholders of the critical infrastructure. This would include dependent entities, governments and the society which the infrastructure serves. The elaboration of this framework is an ongoing work within IMPROVER, where the intention is that the framework will be able to incorporate the results from the assessment methodologies discussed here.

The idea of implementation of indicators to critical infrastructure, and a comparison of indicators, requires that the methodologies are aiming to achieve the same goal, which they are not. Some of the identified methodologies focus on organisational resilience as opposed to critical infrastructure resilience, whereas others focus on other domains of resilience. The output of all of the methodologies is also expressed differently and the question remains what should be done with the calculated resilience of the critical infrastructure.

Of the seven methodologies, based on a set of criteria described in Table 1, three methodologies were shortlisted, namely CIRI, BRT and CIRE. The evaluation based on these criteria is inspired by the work of Prat et al. (2014).

In the next subsections, the three selected methodologies are briefly described. As mentioned earlier, these are mainly resilience analysis methodologies since resilience evaluation is not comprehensively covered. However, we refer to the selected methodologies as resilience assessment methodologies.

Table 1. Selection criteria.

No.	Criteria
1	The methodology shall have features relevant to one or more of the expected impact for the European Commission research topic 'Crisis and disaster resilience – operationalising resilience concepts (DRS-07–14)
2	The methodology shall be applicable to all types of CIs.
3	The methodology shall take cascading effects into account.
4	The methodology shall apply within all resilience domains, either one by one, or altogether.
5	The methodology shall provide qualitative, quantitative and semi-quantitative assessments.
6	The methodology shall be user-friendly and low-cost.
7	The methodology shall provide self-audit.
8	The methodology shall supply already existing practice for risk or resilience management.
9	The methodology shall include individual components (assessments/inventories) with different hazards, safety targets, design lifetimes etc.
10	The methodology shall provide a sufficient balance between complexity and simplicity, as well as between specificity and generality.
11	The methodology shall balance the level of resilience that CI is exposed to, with the level of resilience operators that society are willing to accept.
12	The methodology shall provide relative resilience measurements, e.g. by monitoring own resilience over time, or comparing own resilience to other Cis.

3.1 *Critical Infrastructure Resilience Index (CIRI)*

CIRI is developed within the IMPROVER project. The methodologies use the definition of resilience from UNISDR (2009), as already described. The main aim of the methodology is to provide a 'holistic, easy-to-use and computable methodology to evaluate critical infrastructure resilience' (Pursiainen, 2017). According to the author and developers, the methodology is 'applicable to all types of critical infrastructure, including a possibility to tailor it to the specific needs of different sectors and facilities as well as hazard scenarios.' The methodology also covers all three domains that are being studied in the IMPROVER project, namely technological, organisational and societal. One of the advantages with the methodology is that it is developed as a potential self-auditing tool for CI operators individually, or by CI operators and authorities in cooperation.

The methodology consists of four levels of hierarchically organised indicators. The first level, Level 1, reflects the different phases in the crisis management cycle, illustrated in Figure 1.

The structure of the CIRI is presented in Figure 2, illustrating the different levels and different steps in the methodology. The first step is to establish the context and to collect data. This implies a detailed description of the scenario, including factors such as domain, hazard and situational factors. The next step is to define and select relevant indicators at Levels 2, 3 and 4, where Level 4 is quantitative, semi-quantitative and/or qualitative data which are transformed through a maturity scale, based on the COBIT 4.1 model (COBIT, 2007). The maturity scale is divided into six levels, from 0 to 5, where 0 is non-existent and 5

Figure 1. Targeted resilience adapted from the crisis management cycle (Pursiainen et al., 2017).

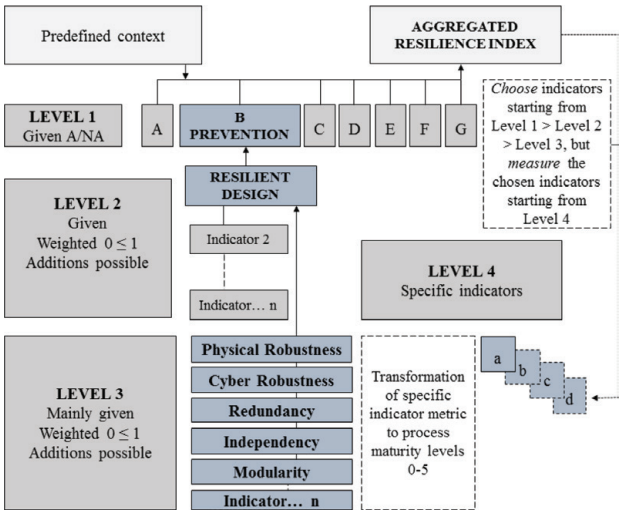

Figure 2. CIRI overall scheme (Pursiainen et al., 2017).

is optimised. Specific metrics of any indicator are transformed into processes, procedures, series of action, series of operations, schemes and methods or systems, corresponding to one of the maturity levels. After determining the maturity levels and weighting factors of all Level 4 indicators, one can estimate the overall resilience by weighted aggregation of the indicators, going upwards from Level 4 to Level 1. Alternatively, one can focus on single indicators at different levels. The level of resilience may be presented in a radar chart, comprising the seven Level 1 indicators, as illustrated in Figure 2.

3.2 *Benchmark Resilience Tool (BRT)*

The Resilient Organisations (ResOrg) in New Zealand developed the Benchmark Resilience Tool. ResOrg uses the following definition of resilience: 'Resilience is the ability of an organisation to survive a crisis and thrive in a world of uncertainty.' BRT is based on the Relative Overall Resilience (ROR) model, developed by McManus et al. (2008), where organisational resilience is defined as 'a function of the overall situation awareness, management of key-stone vulnerabilities, and adaptive capacity of an organisation in a complex, dynamic, and interdependent environment.'

Clearly, BRT is developed for the organisational resilience domain, and can be characterised as a survey tool designed to help measure the resilience of an organisation. In addition, the tool has the ability to measure progress over time, and to compare strengths and weaknesses in resilience against other organisations within the same sector or of a similar size. By measuring and evaluating organisational resilience, BRT contributes to four key organisational needs: the need to demonstrate progress toward becoming more resilient; the need for leading, as opposed to lagging, indicators of resilience; the need to link improvements in organisational resilience with competiveness; and the need to demonstrate a business case for resilience investments.

In the same way as CIRI, BRT is a self-administrated tool. However, BRT also has the feature of being consultant administered. The tool is a questionnaire that provides organisations with an indication of their performance for each of the 13 areas of organisational resilience, described in Figure 3. By executing the questionnaire several times during a time period, it is possible for the organisation to compare and assess the results in order to make improvements. The questionnaire exists in two different versions; one for senior managers and one for staff members. BRT, based on the behavioural elements presented by Ahmad et al. (2015), describes resilience with three independent attributes, building Business As Usual effectiveness as well as robust and agile response and recovery over crisis, namely: leadership and culture; networks; and change ready processes. Furthermore, these three attributes are described using 13 indicators, illustrated in Figure 3, which again may be categorised within two factors: planning and adaptive capacity.

The full survey questionnaire consists of 53 questions and can be administered online, over the phone or as a paper-based survey. All of the 53 items within the BRT model are four-point Likert-scale questions that assess the organisations' agreement with individual statements. After completing the survey, scores are used to analyse the questions—requiring factor analysis with statistical tools for correct interpretation. Results from the analysis, consisting of overall resilience scores, utility-specific resilience scores, lifeline-specific question responses, top crisis data, and staff/human resource data, can be used to evaluate the organisation's scores against general organisations' resilience scores. The results may be presented

Figure 3. The Benchmark Resilience Tool is built up of three organisational resilience attributes and 13 indicators (Adapted from Lee at al., 2013).

graphically to determine where the organisation scores relative to other organisations that have also participated and show average resilience indicator scores for each defined utility group in the results.

3.3 *Guidelines for Critical Infrastructure Resilience Evaluation (CIRE)*

CIRE is developed by the Italian Association of Critical Infrastructure Experts (AIIC) (Bertocchi et al., 2016), who define infrastructure resilience as 'the ability to reduce the magnitude and/or duration of disruptive event. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.' The developers state that CIRE is developed in order to evaluate to which extent the specific infrastructure system is resilient, and why the infrastructure system has a certain degree of resilience. In the same manner as CIRI, CIRE can be customised and applied to any type of infrastructure systems, and the basic questions addressed are:

- Resilience of what?
- Resilience to what?
- Resilience for whom?

The model is structured into four levels and is suitable for both *resilience evaluation* and *resilience engineering*, where resilience evaluation is referred to as 'the overall activities of modelling, and analysis of critical infrastructure system aimed to evaluate the ability to prevent, absorb, adapt, and recover from a disruptive event, either natural or man-made,' and resilience engineering is 'the overall activities of design, construction operation, and maintenance of critical infrastructure system aimed to ensure the ability to prevent, absorb, adapt and recover from disruptive event, either natural or man-made.' The structure of the model is illustrated in Figure 4, where level 1 indicates the four resilience dimensions, Level 2 the four resilience capabilities, Level 3 represents specific features and ultimately Level 4 represents the sector-specific resilience indicators consisting of physical and logical indicators. The CI can be evaluated from a totality point of view through enterprise location to a single process, allowing analyses of different aspects of the infrastructure.

CIRE makes a distinction between logical and physical resilience, and defines logical and physical countermeasures, where logical countermeasures can be both technical and administrative. Associated with physical resilience are features such as redundancy, task separation and advanced technologies. The physical countermeasures are categorised as anti-intrusion, surveillance, fire prevention and extinction and anti-flood measures.

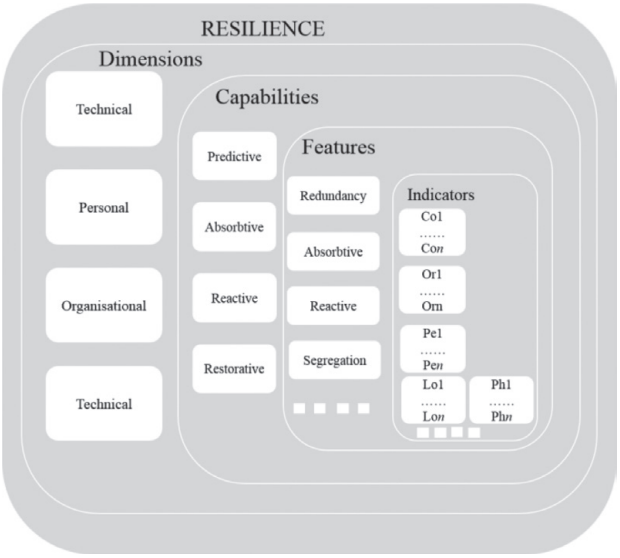

Figure 4. Hierarchical representation of the infrastructure resilience model (Adapted from Bertocchi et al., 2016).

The developers suggest dividing measures for evaluating resilience into three categories: implementation measures, effectiveness/efficiency measures and impact measures.

Data are collected in the same way as in CIRI, with the use of experts. The methodology suggests evaluating resilience using 'Resilience Indicator cards' to estimate the contribution from each indicator to the system in question, either qualitatively, quantitatively or semi-quantitatively. Issues related to weighting and correlation between indicators are not considered in CIRE, but according to the authors, this will be included in future publications. Data emanating from the four dimensions have to be correlated, and a composed value of overall CI resilience is determined by using tailored composing algorithms. The meaning of function f must be determined and a relative weight must be assigned to each factor, R.

$$R_{system} = f(R_{Tech}, R_{PERS}, R_{ORG}, R_{PART}) \quad (1)$$

In the same way as CIRI, the authors suggest the presentation of resilience with a radar chart instead of a single overall value. The resilience associated with a resilience dimension may be estimated by the appropriate value on the radar chart, allowing for a comparison among different charts referring to the same dimension but for different CIs. The methodology begins with answering the initial questions:

- How many dimensions does the evaluation include?

- How many capacities does the evaluation include?
- What is the smallest unit of analysis?
- What Resilience Indicator(s) characterizing the unit under analysis?
- Is the evaluation inductive or deductive?
- Is the evaluation standardised or tailored to the context?

4 DEMONSTRATIONS AND EVALUATION OF RESILIENCE ASSESSMENT METHODOLOGIES

The resilience evaluation methodologies described in section 3 were demonstrated and evaluated with the following process:

1. Demonstration:
   a. Designing case hazard scenarios for each of the four living labs in the IMPROVER project, although this demonstration only includes two of them: the Port of Oslo in Norway; and the Barreiro Water Network System in Portugal.
   b. Selecting a set of resilience indicators relevant to the case scenarios.
   c. Applying each of the methodologies to each of the case scenarios, by using the indicators individually and in combination.

2. Evaluation: The methodologies were compared with regards to a set of desirable criteria for a resilience methodology, as listed in Table A.1 in Appendix A. The evaluation took place in the context of the Design Science Research (DSR) method (Prat et al., 2014).

The following subsections describe the two steps in this demonstration and evaluation process.

4.1 *Demonstration*

4.1.1 *Designing case hazard scenarios*

The cases of the Port of Oslo and the water network in Barreiro are used for illustration and demonstration. In the Port of Oslo case, a termination in the distribution of aviation fuel from the Port to Oslo Airport, Gardermoen, is considered. In the water network case in Barreiro, a severe earthquake is considered, which, among other things, causes a chemical leakage at the SEVESO chemical plant with ensuing dangerous and substantial chemical material leakage (on land and at sea).

4.2 *Selecting resilience indicators*

The three resilience assessment methodologies de-scribed all use a type of index consisting of several indicators. To study the methodologies in more detail, specific indicators, based on the CIRI hierarchy, were selected. The selected indicators, and their respective CIRI levels, are presented in Figure 5. The main criterion for the choice of indicators was their relevance to the designed case scenarios, which were defined as specific events to be evaluated and the primary activity affected by

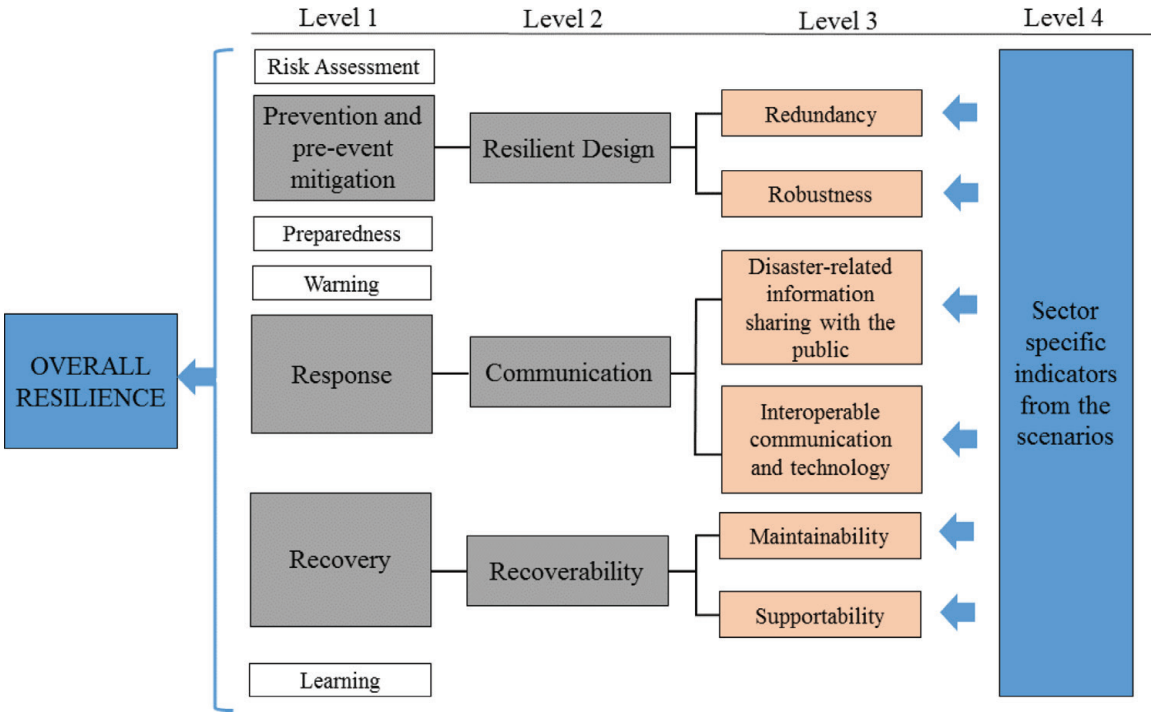

Figure 5. Selected indicators.

the case scenarios. The indicators were selected to cover both post- and pre-activities. Due to time limitations and practical reasons, only a few relevant indicators were selected and evaluated. The selected indicators were also chosen to cover all three domains of interest; technological, organisational and social resilience. For the demonstration of the methodologies in the two scenarios, the cases of the Port of Oslo and the water network in Barreiro, 'redundancy,' 'interoperable information and communication technology' and 'disaster-related information sharing with the public' were selected.

Interoperable information and communication technology can be considered as the ability of Information and Communication Technology (ICT) systems and the business processes they support to exchange data and enable the sharing of information and knowledge. Redundancy is the level of substitutability of a system or system component such that functional service can be maintained. Disaster-related information sharing with the public, directly or via media, is an important task from a crisis management point of view, and it can be expected that a resilience system should have a well-established crisis communication system.

4.3 *Applying the resilience assessment methodologies*

4.3.1 *CIRI*

Port of Oslo

Two main Level 3 indicators were selected for this demonstration: redundancy and 'disaster-related information sharing with the public.' Several Level 4 indicators were chosen based on the scenario described in section 4.2 and presented in Table 2.

For this demonstration, an impact metric for 'Reserve storage capacity' is chosen, which is related to the length of time of the disruption of service. Based on engineering judgements, an impact metric with fictional values based on the COBIT maturity model is developed, as presented in Table 3. In Table 4 fictional maturity levels and weights are assigned.

Finally, the value for the Level 3 indicator 'Redundancy' can be calculated:

$$\text{Redundancy} = [1 \times 0.4] + [4 \times 0.1] + [3 \times 0.3] + [4 \times 0.2] = 2{,}5$$

In order to determine the overall resilience level, the process has to be repeated for all other Level 3 indicators, then Level 2 indicators and finally Level 1 indicators. In Table 5. five Level 4 indicators related to disaster-related information sharing with the public are presented, which again can be described using the maturity process scale.

Table 2. Sector specific Level 4 indicators.

Level 3	Level 4
Redundancy	Reserve storage capacity Alternative means of loading Alternative loading sites Operator cooperation agreement for back-up equipment

Table 3. Impact metric.

Maturity level	Metric (service disruption)	Reserve storage capacity (m^3)
0	90 days	4,600–0
1	30–90 days	45,970–4,600
2	7–30 days	65,360–45,970
3	3–7 days	68,730–65,360
4	3 days	71,260–68,730
5	0	71,260

Table 4. Maturity levels and weighting of Level 4 indicators.

Indicator	Maturity level	Weight
Reserve storage capacity	1	0.4
Alternative means of loading	4	0.1
Alternative loading sites	3	0.3
Operator cooperation for back-up equipment	4	0.2

Table 5. Sector specific Level 4 indicators.

Level 3	Level 4
Disaster-related information sharing with the public	Disaster-related information sharing with the public via traditional means Disaster related information sharing with the public via social media Disaster-related information sharing with the public via SMS Disaster-related information sharing with the public via smartphone applications Disaster-related information sharing with the public via website

'Disaster-related information sharing with the public via social media' is illustrated in Table 6. In Table 7 the level 4 indicators are assigned weights and maturity levels. Based on this, is it possible to calculate the score of the Level 3 indicator 'Disaster-related information sharing with the public.'

Table 6. Description of maturity levels of Level 4 indicators.

Maturity level	Elaborated specific description
0	They do not have social media.
1	Non-disaster-related information is shared with the public via social media.
2	Social media is used to share disaster-related information, but not automatically. There is not a communication strategy and it is up to the individual what sort of information is shared.
3	Social media is used to share disaster related information. A communication strategy exists.
4	Social media is always used to communicate information about disasters. Information is communicated in near real time. Communicating with the public during a crisis is done automatically.
5	Disaster information is shared as in 4, and now the operator has put in place a system with which to respond to the public's question and comments directed to them.

Table 7. Weighting and maturity levels of Level 4 indicators.

Level 4	Maturity Level	Weight
Disaster-related information sharing with the public via traditional means	1	0.2
Disaster related information sharing with the public via social media	1	0.2
Disaster-related information sharing with the public via SMS	0	0.2
Disaster-related information sharing with the public via smartphone applications	0	0.2
Disaster-related information sharing with the public via website	1	0.2

After determining the maturity levels of the indicators subject to analysis, the results can easily be presented in a radar chart.

The water network in Barreiro

For this demonstration we chose the Level 3 indicators 'Interoperable information and communication technology' and 'Disaster-related information sharing with the public.' Starting with 'interoperable and communication technology,' we know that the emergency communication system used at Barreiro is 'Sistema Integrado das Redes de Emergência e Segurança de Portugal' (SIRESP) and we propose as Level 4 indicators the Key Performance Indicators (KPIs) used by the SIRESP Service Level Agreement (SLA), presented in Table 8.

In order to determine the resilience level in the Barreiro scenario, we first need to specify metrics for each Level 4 indicator and each one of the 0 to 5 maturity levels of the COBIT 4.1 framework. With engineering judgement, based on the SIRESP SLA, the maturity levels for availability are specified, as shown in Table 9. The same is done for the four other indicators quite easily. For simplicity, availability only is included. After assigning weights to the indicators, we can calculate the Level 3 indicator.

In order to determine the resilience level, we would have to repeat the process (based on weighted averages) to calculate the values for all other selected Level 3 indicators, then Level 2 indicators and finally Level 1 indicators.

We now demonstrate the Level 3 indicator 'Disaster related information sharing with the public.' Under this Level 3 indicator are a number of proposed Level 4 indicators, as summarised in the Port of Oslo scenario. Using the same qualitative description as the Port of Oslo scenario, and based on the results of a small number of interviews with the operators of the Barreiro municipal water network, the maturity for the organisation in terms of these Level 4 indicators can be identified in the same way as for the Port of Oslo, illustrated in Tables 5–6. In the same way as for the Port of Oslo case, by calculating the level of all the relevant Level 4 indicators, the overall result can be presented in a radar chart.

Table 8. Sector specific Level 4 indicators.

Level 3	Level 4
Interoperable information and communication technology	Availability Coverage Call set-up time Accessibility Audio Quality

Table 9. Maturity levels for Level 4 indicators.

Maturity Level	Metric
0	0%
1	10%
2	50%
3	90%
4	99%
5	99.9%

4.3.2 *BRT*

Port of Oslo

For the following demonstration the indicators 'Prevention and pre-event mitigation,' 'Resilient design' and 'Redundancy' were chosen. In this section, relevant questions from BRT are discussed in association with the scenario and the indicators. The questions referred to is the 53 questions from the questionnaire, which can be found in the reference document (Bertocchi et al., 2016).

In question 9 'Leadership' is highlighted. Planning and organizing for redundancy will be important leadership tasks. Therefore all questions related to leadership will be relevant, albeit not necessarily directly. Question 12 in BRT states that 'Think of all overall highest risks that could lead to crisis or your organisation, please tick the top 5 in the list below.' 'Major accident or fire' were chosen subjectively to be the highest risk in this scenario, and highlight the need for redundancy. Question 13 is related to decision making, where some of its statements are related to redundancy, for instance 'prioritizing customers during reduced capacity.' However, this is a matter for the authorities and not the organisation of the Port of Oslo, since there are regulations to govern certain aspects of the prioritisation of access to fuel. Therefore, this question does not fully capture redundancy.

Question 15 'Effective Partnership' is the question that captures the indicator 'redundancy' and where the answers will have the most impact on overall resilience of the organisation. Five statements are is related to this, for instance 'In a crisis, we have agreements with other organisations to access resources from them.' Question 18 'Internal resources' is about internal resources and can be important for the availability of reserve or back-up solutions (and hence redundancy) within the organisation. Question 19 'Unity of purpose' also touches upon this issue, for instance with the statement 'We understand the minimum level of resources our organisation needs to operate.' Statements related to question 21 'Planning strategies' capture redundancy and the answers have a high impact on the overall resilience, for instance 'We understand the minimum level of resources our organisation needs to operate.' In question 23 the interviewee is asked to tick off plans that the organisation have. A business continuity plan is one alternative, and could involve a plan for redundancy.

The water network in Barreiro

Redundancy was selected as a Level 3 indicator in this example. In the light of the discussion of relevant indicators in the Port of Oslo case, much of the same will be valid for the water network in Barreiro.

4.3.3 *CIRE*

Port of Oslo

In the demonstration of the Port of Oslo case is the indicator 'Redundancy' was chosen, which is one of the resilience features of CIRE. After answering the initial six questions, it is clear that evaluation will include technical, logical and cooperative dimensions, and one capacity, namely absorptive. The smallest unit of analysis is 'Continuity of service,' and for this analysis only one resilience indicator is chosen: Reserve storage capacity. The evaluation is deductive and tailored.

For this scenario two indicators related to redundancy are chosen: 'Reserve storage capacity' and 'Agreements with other organisations to access resources from them,' illustrated in Tables 10 and 11.

The water network in Barreiro

After answering the initial questions, it is clear that this evaluation includes Technical, Logical and Cooperative dimensions. Preventive, Absorptive and Restorative capabilities are included. The smallest unit of analysis is 'Emergency Communication.' For this example we only include the SIRESP availability and the agreements with other organisations. However, we could include many other indicators such as: coverage, call set-up time, accessibility and audio quality. The evaluation is deductive and tailored.

Tables 12 and 13 present examples of resilience indicator cards for the Barreiro scenario.

4.4 *Calculation and presentation of the resilience score*

The methodologies have different ways of analysing the data and presenting the final results. CIRI

Table 10. Example of resilience indicator card.

Lo1 – Redundancy; Reserve storage capacity	
Description	External storage capacity for aviation fuel in order to secure continuity of aviation fuel supply to Oslo Airport Gardermoen during a limited duration of time.
Pertinent dimensions	Primarily technical logical, subordinately Cooperative.
CI Sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Reserve storage capacity affecting the length of time disruption of service
Sources references	Port of Oslo scenario

Table 11. Example of resilience indicator card.

Co1 – Agreement with other organisations to access resources from them	
Description	Alternative loading sites—cooperation with other operators (fuel suppliers) to use their loading sites and equipment during cut-off in their own sites
Pertinent dimensions	Cooperative
CI sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Existence of format cooperation agreements for alterative loading sites
Sources references	Port of Oslo scenario

Table 12. Example of resilience indicator card.

Lo1 – SIRESP	
Description	Alternative loading sites—cooperation with other operators (fuel suppliers) to use their loading sites and equipment during cut-off in their own sites
Pertinent dimensions	Primarily Technical Logical, subordinately Cooperative
CI sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Percentage availability
Sources references	Barreiro scenario

Table 13. Example of resilience indicator card.

Co1 – Agreement with other organisations to access resources from them	
Description	One of the most important factors in the Barreiro scenario is the communication with external partners using SIRESP as the emergency communication system. The system is critical in a crisis situation, but it is also crucial to have agreements that ensure a rapid and effective response with hospitals, police, etc.
Pertinent dimensions	Cooperative
CI sector relevance	To be estimated by the sector specific experts
Evaluation method(s)	Existence of formal cooperation agreements for alterative loading sites
Sources references	Barreiro scenario

uses a radar chart with all the Level 1 indicators. This will depend on the indicators selected and the weighing of the indicators. To gain a picture of the overall resilience, all selected indicators must be evaluated. Considering Level 3 indicators as 'Redundancy' and 'Disaster-related information sharing with the public,' they will only contribute to one of the Level 1 indicators in the radar chart. However, a low score on the Level 1 indicates that effort should be put into improvement.

CIRE also suggests the use of a radar chart to present the results. The methodology is still under development, and there is no clear description of how the resilience score is determined. However, the developers suggest presenting the four different dimensions of resilience in individual radar charts. Hence, the results from the demonstration, with both logical and cooperative indicators, will be presented in two different radar charts. As for CIRI, the final result will depend on the other indicators selected.

BRT suggests presenting the results from the questionnaire graphically for each of the 13 indicators. For the selected indicators in the demonstration, it is a difficult task to show how they contribute to the overall resilience, since there are several questions from the 13 indicators in the methodology that relate to the selected indicators.

5 EVALUATION OF RESILIENCE ASSESSMENT METHODOLOGIES

5.1 *Feedback from demonstrations*

5.1.1 *CIRI*

The CIRI methodology is structured and easy to learn to use. Indicators, evaluation of the maturity levels and the weightings of the indicators can be sector-specific. However, this makes it difficult to compare different scenarios because the Level 4 indicators are not necessarily the same. One of the drawbacks with the methodology is that the maturity model of COBIT was originally designed for processes, not indicators. The metrics are often designed using engineering or expert judgement, which might make the different levels difficult to compare. The same is true for the weighting of the indicators.

5.1.2 *BRT*

The methodology of BRT is simple to learn and use. BRT helps to achieve an overall picture of the organisation, and the results can be compared across infrastructures. However, BRT does not offer a detailed analysis and gives no explanation regarding how to calculate the resilience level.

Moreover, any manager in the organisation, who probably will not have knowledge about the various areas, can answer the questions. BRT focuses on organisations rather than critical infrastructures, and when looking at specific indicators, one can say that BRT is too general. Based on the documentation, it is not clear how to calculate the outcome of the questionnaire.

5.1.3 *CIRE*

The CIRE methodology is general and can be applied to all types of critical infrastructures. When using the methodology, one can monitor individual indicators within different domains. The drawback is the lack of a clear methodology to determine the overall resilience. In its current form, it does not provide a description about this. Moreover, CIRE is sensitive to interpretation and individual evaluations. Thus, it might be difficult to compare critical infrastructures. However, it may be suitable for relative resilience measurements for the same critical infrastructure over time.

5.1.4 *Resilience score*

As highlighted, the methodologies have different ways of analysing and presenting the resilience scores. Within CIRI and CIRE it is quite arbitrary how the different indicators are selected and weighted by the operators, which will then influence the results. In addition, the scales are different in the methodologies. BRT is based on a questionnaire, which gives the results of 13 indicators which are fixed. Hence, it is easier to compare the results between different organisations. The fact that the three methodologies do not evaluate exactly the same thing makes it hard to compare the results. All of the three methodologies end up quantifying the resilience level. However, it is not clear what the results tells us or how the results should be used.

5.2 *Evaluations results*

Based on the demonstrations, qualitative evaluation of the performance of the methodologies against each of the criteria in Table 1 is performed. The evaluation process sums up the performance of each of the methodologies in the different evaluations against the individual criteria. In this way, it is possible to determine how well each methodology fulfils the individual criteria. An overall evaluation is then carried out by summing the ability to fulfil all of the criteria for individual methodologies. The score of the methodologies against each of the criteria is given by the following equation:

$$S_{Ci} = \sum_{\forall evaluations} X_{i,j} w_i \quad (2)$$

where S_{Ci} is the score for how well the methodology fulfils criteria i; $X_{i,j}$ is the assessment of how well the different methodologies fulfil the criteria i in the evaluation j. The weighting w_i represents the importance of each of the criteria in achieving the desired results within the project. Criteria are weighed according to simple low (0.04), medium (0.08) and high priorities (0.17) according to the priority order of the criteria. The scores of the three different methodologies against each of the criteria are summarised in Tables 14–16. These numbers are only intended to give a qualitative indication of the relative performance of each of these methodologies against the different criteria.

5.2.1 *CIRI*

Table 14. Evaluation results.

Criteria no.	Weighting	Demonstration score	Score
1	0.17	0.75	0.13
2	0.17	1	0.17
3	0.17	0.5	0.08
4	0.13	1	0.13
5	0.13	1	0.13
6	0.13	1	0.13
7	0.08	0.6	0.05
8	0.08	1	0.08
9	0.08	0.5	0.04
10	0.04	0.5	0.02
11	0.04	0.33	0.02
12	0.04	0	0

5.2.2 *BRT*

Table 15. Evaluation results.

Criteria no.	Weighting	Demonstration score	Score
1	0.17	0.25	0.04
2	0.17	0.25	0.04
3	0.17	0.75	0.13
4	0.13	0.33	0.04
5	0.13	0.67	0.08
6	0.13	1	0.13
7	0.08	1	0.08
8	0.08	1	0.08
9	0.08	0.25	0.02
10	0.04	0.6	0.03
11	0.04	0	0.00
12	0.04	0.04	0.04

5.2.3 *CIRE*

Table 16. Evaluation results.

Criteria No.	Weighting	Demonstration Score	Score
1	0.17	0.25	0.04
2	0.17	1	0.17
3	0.17	0.75	0.13
4	0.13	0.67	0.08
5	0.13	1	0.13
6	0.13	1	0.13
7	0.08	0.7	0.06
8	0.08	1	0.08
9	0.08	0.1	0.01
10	0.04	0.4	0.02
11	0.04	0	0.00
12	0.04	0	0.04

5.3 *Results according to criteria*

1. All of the methodologies for resilience assessment require more consideration of the expected impacts from the topic description, which are:
   - More efficient uptake of risk assessment through Member States and Associated Countries and Critical Infrastructure Providers.
   - More effective and coherent crisis and disaster resilience management.
   - The methodology shall be useful as a training tool for rescuers.
   - The methodology shall take into account communication and interaction with the public.
2. The applicability of the methodologies to all types of critical infrastructures is notably less well fulfilled in the BRT. However, this is to be expected since it aims at organisational resilience as opposed to infrastructure resilience.
3. Both BRT and CIRE account in some way for cascading effects. In CIRE this is achieved by considering exposure of the organisation to certain other critical services, and is included as an indicator. At present this is lacking from CIRI, however this could be relatively easily included as an additional resilience indicator.
4. CIRI accounts for resilience across the organisational, the social and the technological domains. CIRE accounts for organisational and technological resilience, while BRT only accounts for organisational resilience.
5. CIRE and CIRI allow for qualitative, quantitative and semi-quantitative assessment. The BRT only provides for qualitative assessment.
6. All three methodologies appear to be user friendly and low cost.
7. In terms of self-auditing capability—CIRI requires, for some of the indicators, specialist engineering or other expert judgement. It is however possible to perform a self-audit using CIRI of the higher level indicators. The same is valid for CIRE. BRT provides the greatest capability for self-audit due to the questionnaire nature of the assessment tool.
8. All three methodologies could in principle be linked to existing risk assessment practices. However, this is not elaborated on in any of the methodologies.
9. CIRI could account for the performance of individual components against different hazards. This could be achieved by accounting for component reliability and its impact on the overall asset reliability.
10. The nature of BRT makes it particularly simple to implement.
11. As resilience assessment tools, none of the methodologies offer a means to balance the level of resilience that the CI has with the level of resilience operators and society are willing to accept.
12. Only the BRT has as part of the methodology an explicit consideration of comparisons with the resilience of other organisations over time.

6 CONCLUSION

The feedback from the demonstration and evaluation of the three methodologies is mixed. All methodologies have pros and cons. Moreover, there seems not to be any strict objective way to evaluate the methodologies, but much depends on what one wants to do with a resilience assessment methodology, how much effort and time, and who is doing it. All the methodologies end up quantifying the resilience with a final score. However, what the score actually means is dependent in the interpretation of the end user, and there is no clear guidance on how the result should be used to improve the resilience. The demonstrations and the evaluation have identified the pros and cons with the different methodologies and given valuable insight in what properties the subsequent phases in the IMPROVER should aim to include.

These notions lead to the conclusion that the IMPROVER project should aim at developing a CI resilience assessment framework which is well defined but which at the same time also includes the possibility of flexibly to account for idiosyncrasies of the different type of CIs and their operators. Such a general framework for resilience assessment of CIs should remain compatible with the current guidelines for risk assessment of the Member States and should integrate the paradigm of resilience into the risk assessment process according to ISO 31000.

This differentiation between a resilience assessment framework and a resilience analysis methodology would account for the first criteria identified above—those related to the efficient uptake of risk assessments in the Member States as well as more effective and coherent crisis and disaster resilience management. The adoption of a resilience methodology into such a resilience assessment framework would also address many of weaknesses or shortcomings in existing resilience analysis methodologies.

ACKNOWLEDGEMENTS

The article is a product of the IMPROVER project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 653390.

REFERENCES

Ahmad, R. et al., 2015. A supply chain resilience maturity model. Conceptual paper. Available at: http://ir.canterbury.ac.nz/handle/10092/11044 [Accessed 14 November 2016]

Australian Government. http://www.organisationalresilience.gov.au/HealthCheck/Pages/default.aspx. [Accessed: 14 November 2016]

Bertocchi., G., Bologna, S., Carducci, G., Carrozzi, L., Cavallini, S., Lazari, A., Oliva, G., and Traballesi, A., 2016. Guidelines for Critical Infrastructures Resilience Evaluation. Associazione Italiana esperti Infrastrutture Critiche (AIIC) – Italian Association of Critical Infrastructures Experts. Technical Report. DOI: 10.13140/RG.2.1.4814.6167

COBIT 2007. *Cobit 4.1 Excerpt. Executive Summary Framework*. United States of America: IT Governance Institute. [Online] Available from: https://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT4.pdf

Hollnagel, E., 2010. How resilient is your organisation? An introduction to the Resilience Analysis Grid (RAG). Sustainable Transformation: Building a Resilient Organization, May 2010, Toronto, Canada. http://www.unisdr.org/we/inform/terminology

ISO 2009. *Risk management.* International Standardization Organization. IEC/FDIS 31000

Lee, A., Vargo, J., and Seville, E., 2013. "Developing a Tool to Measure and Compare Organizations' Resilience." Nat. Hazards Rec., 10.1061/(ASCE)NH.1527–6996.0000075, 29–41.

Peffers, K., Tuunanen, T., Rothenberger, M. A. and Chatterjee, S., 2007. A design science research methodology for information systems research. Journal of Management Information Systems, 24 (3), 45–77.

Prat, N. et al., 2014. Artifact Evaluation in Information Systems Design-Science Research – a Holistic View. Proceeding of the 19th Pacific Asia Conference on Information Systems (PACIS).

Prior, T. (2015) *Measuring Critical Infrastructure Resilience: Possible Indicators.* Risk and Resilience Report 9. ETH Zürich: April.

Pursiainen, C.H., Rød, B., Baker, G., Honfi, D. and Lange, D., 2017. Critical Infrastructure Resilience Index. CRC Press 2017 ISBN 9781138029972.p 2183–2189.

UNISDR 2009. *UNISDR Terminology on Disaster Risk Reduction*, United Nations International Strategy for Disaster Reduction (UNISDR), Geneva, Switzerland, May 2009. [Online] Available from: http://www.unisdr.org/we/inform/terminology

Paper IV

Novel methodologies for analysing critical infrastructure resilience

Storesund, K., Reitan, N. K., Sjøstrøm, J., Rød, B., Guay, F., Almeida, R., Theocharidou, M. (2018).

Published in Haugen et al. (Eds.), *Safety and Reliability – Safe Societies in a Changing World. Proceedings of the 28th European Safety and Reliability Conference, ESREL* (pp. 1221 – 1229). London, UK: Taylor & Francis Group. ISBN 978-0-8153-8682-7.

Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds)

Novel methodologies for analysing critical infrastructure resilience

K. Storesund & N.K. Reitan
RISE Fire Research, Trondheim, Norway

J. Sjöström
RISE Research Institutes of Sweden, Borås, Sweden

B. Rød
UiT The Arctic University of Norway, Tromsø, Norway

F. Guay
INOV INESC Inovação, Lisbon, Portugal

R. Almeida
Danish Institute of Fire and Security Technology, Hvidovre, Denmark

M. Theocharidou
European Commission, Joint Research Centre, Ispra, Italy

ABSTRACT: In the field of Critical Infrastructures (CI), both policy and research focus has shifted from protection to resilience. The IMPROVER project has developed a CI resilience management framework (ICI-REF), applicable to all types of CI and resilience domains (technological, organisational and societal) allowing operators to understand and improve their resilience. IMPROVER has also developed methodologies to be used within the framework, accompanied with resilience indicators for operators to assess their technological and organisational resilience. The framework allows CI operators to incorporate resilience management as part of their risk management processes. The ICI-REF, the resilience analysis methodologies and indicators have been optimised, applied and demonstrated in a pilot implementation, focusing on the potable water supply in Barreiro, Portugal. Conclusions from the operators so far are that the indicators, well-defined and unambiguously described, are crucial for monitoring resilience activities, to ensure objective, consistent, repeatable and representative results from the assessed processes.

1 INTRODUCTION

Increasing Critical Infrastructure (CI) resilience is one is one of the main objectives for the European strategy towards a more secure Europe (COM, 2010). Through the Program for Critical Infrastructure Protection (EPCIP), issues and approaches to focus on are defined, where measures to facilitate implementation of resilience concepts to CI are identified (SWD, 2013). The concept of resilience has evolved from ecological resilience, via psychology, engineering to the disaster risk reduction field. There is thus a range of definitions of the concept of resilience and for this context we use that of UNISDR *"The ability of a system, community or society exposed to hazards to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions"* (UNISDR, 2009). In EU, CI is defined as: "*an asset, system or part thereof located in Member States which is essential for maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*" (Council, 2008).

An overall goal of the EU-funded Horizon 2020 project IMPROVER is to improve European CI resilience to crisis and disasters, through the implementation of technological, organisational and societal resilience concepts. To that end, the IMPROVER Critical Infrastructure REsilience Framework (ICI-REF) was developed. The framework is supported by resilience analysis methodologies and indicators, also developed in IMPROVER. It is inspired by existing stand-

ards and frameworks e.g. ISO 31000, ISO 22301, ISO 22316, Org. Resilience HealthCheck (Austr. Government, 2017), Benchmark Resilience Tool (Resilient Organisations, 2014) and Resilience Measurement Index (Petit et al, 2013).

To ensure that the developed ICI-REF framework, with supporting methodologies and indicators, is fit-for-purpose, it is optimised in pilot implementations, by application to relevant scenarios in semi-real environments at several living labs. One pilot implementation has recently been conducted, focusing on potable water supply in Barreiro, Portugal.

This paper describes structures and processes of the ICI-REF and resilience analysis methodologies, including preliminary results of the pilot implementation at the Barreiro living lab, Portugal.

2 IMPROVER CRITICAL INFRASTRUCTURE RESILIENCE FRAMEWORK (ICI-REF)

2.1 *The ICI-REF structure and process*

ICI-REF is a general and well-defined framework for managing the technological, organisational and societal resilience of CI (Lange et al., 2017a; 2017b). It includes the flexibility to account for the unique features of the various types of CI, giving CI operators an understanding of, and a capability to improve, their resilience. The framework extends standard risk procedures (ISO 31000) and considers resilience assessment as complementary to risk assessment. The framework is constructed such that it is easily incorporated within existing risk management processes by CI operators. Initial feedback by CI operators (Theocharidou et al., 2016) indicated this approach as the most feasible one, as it can improve their current practices and allow for risk and resilience management decisions to be taken based on the results of both assessments. ICI-REF allows operators to perform self-assessment or focused analysis of technological/organisational aspects in order to either monitor resilience over time, or compare to similar CI within the same sector. The ICI-REF structure is depicted in Fig. 1.

The ICI-REF process starts with *establishing the context*, implying the gathering of information, defining the resilience domain(s), etc. The defined context, risk identification and risk analysis are then fed into, and complemented by, the resilience assessment process. *Resilience assessment* comprises of *resilience analysis* and *evaluation* against pre-defined criteria. Three different resilience analysis methodologies have been developed (described in 2.3). The results from risk and

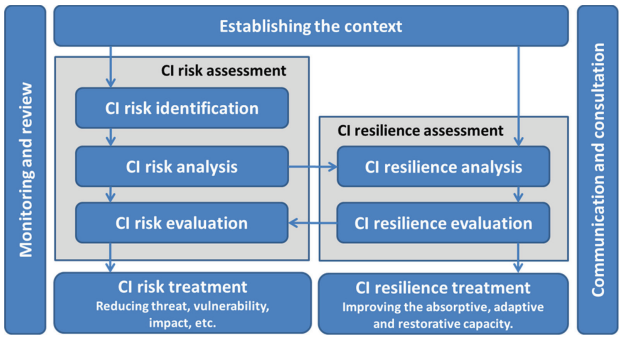

Figure 1. Structure of the IMPROVER Critical Infrastructure REsilience Framework (ICI-REF).

resilience assessments constitute the basis for designing treatment plans, describing how to both mitigate risk and improve resilience. This parallel process allows decision makers to select risk and resilience measures in a cost-effective way, especially when a measure can be implemented to address both risk and resilience objectives. Throughout the ICI-REF process, *Monitoring and review* as well as *Communication and consultation* are continuous background processes (see Lange et al., 2017).

CI resilience analysis can be performed by implementing existing methodologies, or by methodologies developed in IMPROVER. This paper focuses on technological and organisational resilience analysis, for which resilience assessments are performed at the CI level. Assessment and management of societal resilience shall instead be conducted on regional or national levels, using CI resilience assessments as input. A modified version of ICI-REF is developed for this purpose (Rosenqvist et al., 2018).

2.2 *Resilience indicators*

In the context of IMPROVER, the term "resilience indicators" is related to variables that can be used, either alone or in combination, as a representation of resilience. Qualitative, semi-quantitative or quantitative indicators are analysed and, when sufficient, aggregated to a measure of resilience.

The resilience indicators should be clearly defined, in order to ensure objectivity and a proper balance between generality and specificity. To monitor resilience over time or comparing to similar CI, the indicators must also provide reproducibility and repeatability. Measurement scales for the indicators and their possible weight factors should ideally be benchmarked at a sectoral level.

Based on literature and defined requirements from CI operators associated with IMPROVER, the resilience indicators to be included in the resilience analysis step of ICI-REF are developed and optimised. They relate to the various resilience

analysis methodologies used for different resilience domains.

2.3 *Resilience assessment*

As a first step, the CI operator may want to conduct an initial self-assessment to indicate strengths and weaknesses in its resilience; i.e. in which areas or domains a more in-depth assessment is required. For this purpose, the operator may find a resilience analysis methodology with high flexibility useful, such as the Critical Infrastructure Resilience Index (CIRI) developed in IMPROVER (Pursiainen et al., 2017).

This process may be sufficient, but if required, operators can perform re-assessment by using analysis methodologies which goes more into details. For this purpose, two different methodologies have been developed: the IMPROVER Technological Resilience Analysis (ITRA) and IMPROVER Organisational Resilience Analysis (IORA) for analysing technological or organisational resilience, respectively (Bram et al., 2017; Mindykowski et al., 2016). CIRI, ITRA and IORA methodologies are briefly described below.

2.3.1 *Critical Infrastructure Resilience Index (CIRI)*

Critical Infrastructure Resilience Index (CIRI) is a holistic and easy-to-use self-assessment methodology. It is applicable to all types of infrastructures, and built on a four level hierarchy of indicators, focusing mainly on the technological and organizational domain. The backbone for CIRI is the crisis management cycle (OECD, 2011; Pursiainen, 2017). The different phases in the cycle corresponds to the seven Level 1 indicators: Risk assessment, Prevention, Preparedness, Warning, Response, Recovery, and Learning, Fig. 2. Under each Level 1 indicator there is a subset of given generic indicators (Level 2).

Further, for each Level 2 indicator there is a new subset of mainly given, measurable indicators. However, as sectors use different metrics and measures (quantitative/qualitative) the exact measurement depends on the sector, referred to as Level 4 indicators, the bottom of the hierarchy.

For a common viewpoint, Level 4 indicators are transformed to qualitative maturity scale, scaling, from 0 to 5. At Level 3 and 4, the operator has the possibility to assign weight to the indicators according to their importance. After assessing the Level 4 indicators, results are aggregated up the hierarchy, and each Level 1–3 indicator get a score from 0 to 5. The result is presented in a radar chart with all the seven Level 1 indicators.

In addition, to present a more detailed analysis, it is possible to construct charts for all Level 1 over their respective Level 2 indicators, see Fig. 3.

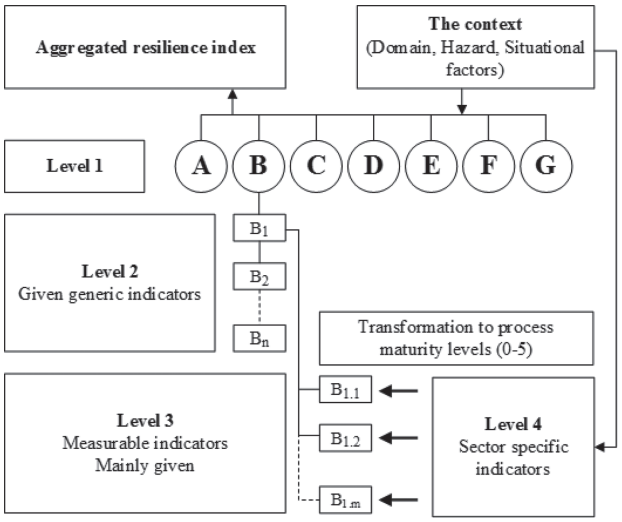

Figure 2. The hierarchical structure of Critical Infrastructure Resilience Index (CIRI). The Level 1 indicators, representing different phases in the risk management cycle, are here denoted (A) Risk assessment, (B) Prevention, (C) Preparedness, (D) Warning, (E) Response, (F) Recovery and (G) Learning.

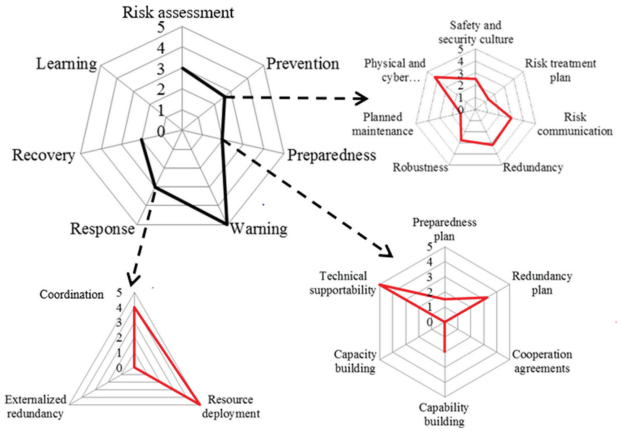

Figure 3. Analysis results for most Level 1 indicators, and Level 2 indicators under Prevention, Preparedness, and Response.

It should be noted here that this is a self-assessment methodology and thus not fully objective. However, the result is indicative of the CI's resilience level and highlights strengths and weaknesses of the infrastructure, both from the technological and organisational perspective. It can be used as the basis for further detailed analysis, using methodologies like IORA and ITRA.

2.3.2 *IMPROVER Technological Resilience Analysis (ITRA)*

Technological resilience is often visualised using the performance loss and recovery function or the area between the function and an uninterrupted capacity/performance. From the risk identification,

Fig. 1, a prioritised list of possible hazards which could impact the CI is used as input to the technological resilience analysis, which aims at quantifying the performance loss and recovery of the CI service. Thus, technological resilience is conditional on the occurrence of a specific hazard, following the procedure of the risk management of ISO 31000.

Estimating the functionality needs therefore suitable *intensity measure* of the hazard to which the vulnerability of the system's subparts can be evaluated through their *fragility.* Combining this information gives a measure of the *damage* to the system which should be transformed into one or several *performance measures* in order to focus on the core aspect of resilience: functionality of the system.

Once the performance measures loss and recovery functions are estimated they should be evaluated against other CI, historical performance or the needs and expectations of the infrastructure's end-users. It is therefore of vital importance to choose the performance criteria keeping in mind that: (i) they should be possible to translate from estimated damages, with sufficient accuracy and (ii) they should be constructed such that they can be compared to other CIs, historical performance or (preferably) the needs and tolerances from the end-user (Petersen, 2018).

2.3.3 *IMPROVER Organisational Resilience Analysis (IORA)*

IORA follows a similar structure to other organisational analysis methods. The purpose of the analysis is promoting resilient performance. Subsequent levels are functions, forms and processes which contribute to this purpose. The functions required to achieve this are: design of tasks and roles; design of the framework and its content, goals, rules, processes and procedures; strengthening collaboration; learning and redesign; underlying values and interpretations, Fig. 4.

Organisational resilience analysis process requires collection and processing of information about how the organisation's processes contribute to this. For the Barreiro implementation this is done via in-depth interviews based on a narrative of a historical event (saline intrusion in a fresh water well). Functions, forms and processes during this event form the basis for the analysis and the subsequent evaluation.

3 PILOT IMPLEMENTATION ON POTABLE WATER SUPPLY NETWORK

3.1 *Test object*

The object to be tested in the pilot implementation, comprises of the ICI-REF, its supporting methodologies for resilience analysis (CIRI, IORA and ITRA) and the developed resilience indicators. The test object will be denoted as ICI-REF in the remainder of the document for simplicity.

3.2 *Living lab: The potable water supply system of Barreiro*

Barreiro's municipality, with an area of 36.41 km^2, has, according to the Census 2011, a population of 78,764 people. It has 17 km river front to Tagus and Coina rivers and an important road-rail-river terminal. It is located about 40 km from Lisbon to which it is linked by two bridges, and about 35 km from Setúbal, the district capital. Barreiro's potable water supply system consists of 11 licensed ground-water intakes from a semi-confined aquifer, 7 reservoirs for treated water storage with the total capacity of 12.750 m^3, 7 treatment installations, for disinfection with the addition of sodium hypochlorite, 3 pumping stations, 5 blowers, 16.1 km of main ducts, and 308 km of meshed distribution pipes.

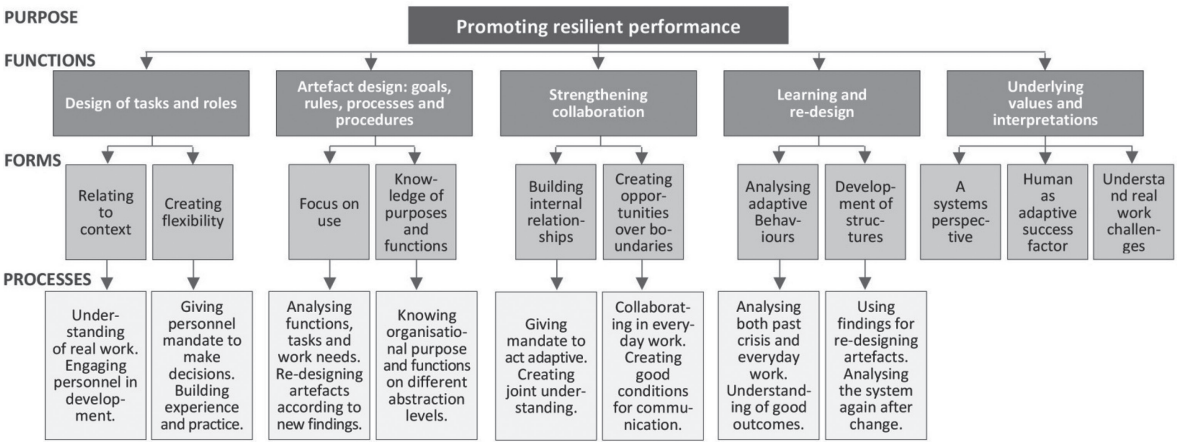

Figure 4. Indicators on different abstraction levels in the IMPROVER Organisational Resilience Analysis methodology (IORA).

The municipality has a remote management system that allows real time monitoring of pressure and flows in the water supply (and waste water) systems. The pilot implementation focuses on three pressure zones in the north, which combined account for 60% of the total water supply in the municipality.

Fig. 5 shows the area subject to the assessment.

3.3 *Systematic approach for testing and evaluating the performance of ICI-REF*

To make the pilot implementation robust, a triangular approach was used for testing and evaluating the performance of ICI-REF. Triangulation is the combination of two or more data sources, investigators, methodologic approaches, theoretical perspectives or analytical methods within the same study (Denzin, 1970; Kimchi et al., 1991). Using multiple methods decreases the "deficiencies and biases that stem from any single method" (Mitchell, 1986) creating "the potential for counterbalancing flaws or the weaknesses of one method with the strengths of another." Therefore; focus group, documentation, field studies and surveys were used to collect data for the critical evaluation of the performance of ICI-REF. The IMPROVER project embraces all these approaches in several steps and iterations for optimising ICI-REF.

3.3.1 *Collection of data*

A *focus group,* consisting of representatives from the operator at the Barreiro living lab, was selected based on their insight into current processes and methodologies for risk assessment at the Barreiro living lab. There has been close cooperation between the focus group and the project team throughout the project via continuous communication, and workshops. These were invaluable in addressing strengths and weaknesses of ICI-REF before the final pilot implementation. The focus group, as a qualitative, exploratory research method, has aided the understanding about not only the operators' opinions, but also how and why they think the way they do.

Field studies were performed for testing the application of ICI-REF in a semi-real environment. Field studies require detailed observation and evaluation, allowing conclusion of understanding and comparisons of the information generated from each site (Burgess, 1984; Denzin & Lincoln, 2011; Rossman & Rallis, 2011). An advantage of field studies is that they give better external validity than in laboratory experiments because a field experiment takes place in typically occurring social settings.

The field study relied on application of ICI-REF to a relevant hazard scenario. A scenario with high disaster risk was prioritised by structured expert judgement elicitation by the stakeholders. Fig. 6 shows a hazard map for the Barreiro living lab.

The hazard chosen to assess the resilience of the water supply system was an earthquake with liquefaction, which is considered the highest disaster risk for the water network combining consequence and probability. The assets susceptible to the hazard are:

– The reservoir, pipe system, pumps and the critical users being the hospital and the health centre.
– All technical equipment used to repair and to distribute redundant functionality.

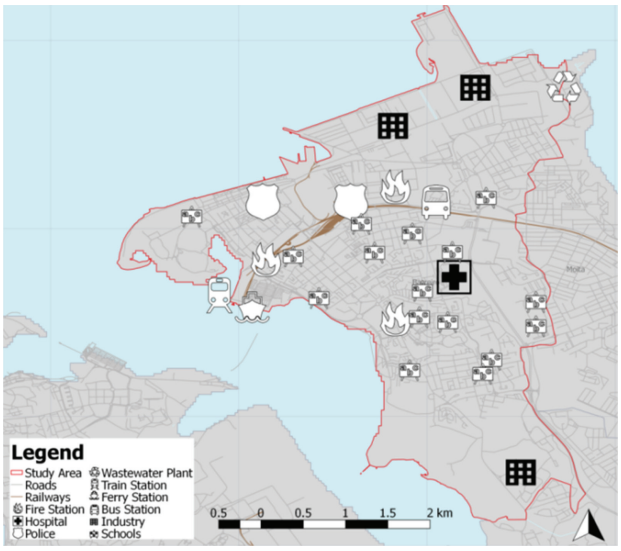

Figure 5. The northern part of the Barreiro municipality subject to the pilot implementation.

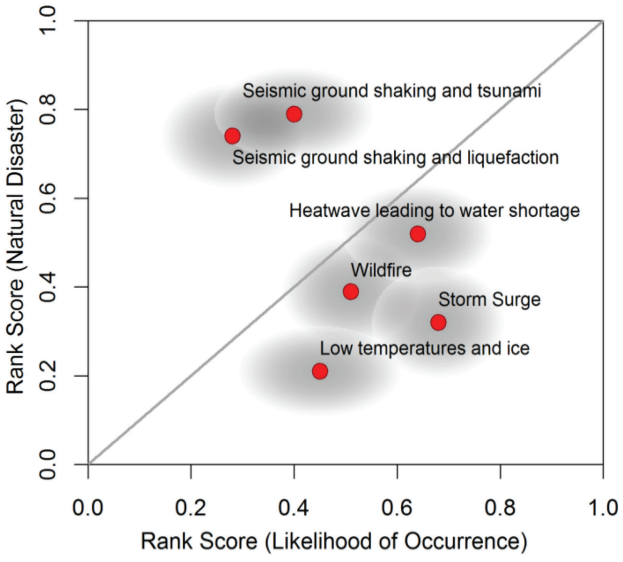

Figure 6. Plot of rank scores of six natural hazard scenarios based on their likelihood to cause disaster and to occur at Barreiro's water network in the next 5 years. (Pursiainen et al., 2015).

All staff and the entire organisation and the processes used in the preparatory, functional and administrative work.

Documentation was collected in order to analyse vital data from the CI. For example, the safety plans, and organisation chambers. These documents were used to assess the as-is situation of the CI. Typically, the analysis aims at visualising the current state process to clarify how the CI process works today, and what can be done to improve the current situation.

Different forms of *surveys*, aimed at the operator, project team members and other stakeholders were used in advance, during and after the pilot implementation. By using surveys, a broad range of data has been collected, e.g. tolerance levels; attitudes; opinions; beliefs; values; behaviour and factual. The surveys were used as basis both for defining performance criteria for resilience assessment and for the critical evaluation of the performance of ICI-REF.

3.3.2 *Critical evaluation*

Eighteen success factors were developed for the critical evaluation of the performance of ICI-REF. These ensure that ICI-REF meets stakeholders and end-users needs and are designed based on continuous input from the living labs during the project. The design science research methodology (Hevner et al., 2004) is used for the critical evaluation process in which the success factors are evaluated based on demonstration results and applications of ICI-REF.

The defined success factors of the project are primarily designed for critical evaluation of the overall ICI-REF framework, but they also implicitly set requirements to the relevance and quality of the tested analysis methodologies with indicators. Examples of success factors related to indicators are shown in Table 1.

3.4 *Results from initial demonstrations*

CIRI, IORA and ITRA were all applied in the initial demonstrations. Evaluation from ITRA showed that the system most probably will meet the expectations of end-users for reasonable scenarios of damage. Also, despite being highly dependent on key personnel resources the flat organisation helps in fast recovery in times of crises, as shown in IORA evaluation.

A set of resilience indicators was tested within the CIRI methodology and assessed, using a software tool developed in IMPROVER (accessed at: http://improver-inov.herokuapp.com/). The indicators were discussed and evaluated by the operator according to the indicators' relevance and comprehensibility as means of assessing their resilience.

Table 1. Examples of success factors for critical evaluation of the relevance and quality of resilience indicators.

Success factor	Defined by
The framework shall be applicable to all types of CI	The balance and definitions of indicators
	Clearly described and categorised indicators
The framework shall be easy to use	Guidance on how framework indicators can be interpreted in relation to resilient performance
The framework shall provide effective and coherent crisis and disaster resilience management	Resilience indicator follow-up should promote a shared view within the organisation on real work challenges.
The framework is arranged for being revised continuously	Existence of a system for recurring analysis, criticism and revision of the indicator framework and implementation

Table 2. Scale for analysing perception of indicators by the Barreiro operator.

Rating	Definition
A	The indicator was perceived, and there is evidence of the indicator
B	The indicator was perceived, but there is no evidence of the indicator
C	The indicator was not perceived
D	Not applicable

The operator was asked to assign resilience measurement scores to the indicators, and to rate them on the perception scale, according to how well they were understood by the operator. The scale for the perception ratings is presented in Table 2.

The structure and processes of resilience analysis methodologies proved functional in the demonstration. Based on the feedback from the operator, only minor modifications of the methodologies were required to optimise the relevance of the analysis results towards the main pilot implementation. The operator expressed the need for user-friendly, clear and not too complex assessments. They further concluded that the structure is not the main point of interest to the living lab, but the functionality of the assessment process, and the questions and goals related to the indicators. An issue pointed out by the living lab is which resources are required to perform the assessment; i.e. whether they need to employ external resources or can train internal resources.

The operator emphasised the crucial role of resilience indicators in the monitoring of resilience activities. However, to ensure objective, consistent, repeatable and representative results, the indicators and their designed questions must be defined using unambiguous terms. As long as the indicators are well described and leave little room for subjectivity, the high number of indicators is not a problem. The need for guidelines was also expressed.

Challenges related to the definitions of measurement scales and assignments of weights for qualitative or semi-quantitative indicators were pinpointed. E.g. the measurement scale used to assess the indicators should be well-defined since it is mandatory to understand the differences between the different measurement scales to perform benchmarking. It was also discussed how flexible the indicator structure should be; e.g. if CI operators shall be allowed to define their own scales and weights, and how this will affect the assessments and limit their relevance.

The perception of the operator that some of the indicators were too vague, needed to be better explained and that some were difficult to point out evidence for, led to adjustments and development of the overall set of indicators and how they are presented.

To address the need for proper descriptions and definitions of sector-specific indicators, "indicator cards" were developed for the complete developed set of technological and organisational resilience indicators at the lower CIRI level. Each individual resilience indicator card provides a detailed description of the sector-specific indicator subject to assessment as exemplified in Fig. 7.

The indicator cards consist of the following information:

- The assessed indicator and its parent indicators are listed.
- Detailed information about the context is given. The resilience domain (technological or organisational), hazard types (natural, non-malicious man-made, malicious man-made and multi-hazards) and situational factors (e.g. temporal, geographical or conceptual considerations for taking such an indicator into account) are indicated. Finally, the applicable sector (in this case potable water supply) is pointed out and if the indicator is generic or scenario specific.

A description of the indicator and guidance for assessing the maturity level is provided through a rationale of why this indicator is justified. Moreover, a question is provided, which can be asked to the operator for measuring the indicators in a clear and explicit manner with the 6 different maturity levels described (scale 0–5) and a reference for describing the indicator.

Resilience indicator card		
Level 1	Response	
Level 2	Communication	
Level 3	Interoperable information and communication technology	
Level 4	**Availability (SIRESP)**	
Context		
Domain	Technological/Organisational	
Hazard Type	General	
Situational factors	N/A	
Applicable sectors	Water Supply	
Generic or scenario specific	Generic	
Indicator description and assessment		
Rationale	SIRESP is the emergency communication system used in Barreiro, and it is crucial for effective coordination and exchange of information during emergency periods.	
Question	What is the availability level of the SIRESP system?	
Answer modalities	0	0-1 %
	1	1-10 %
	2	10-50 %
	3	50-90 %
	4	90-99 %
	5	>99 %
References	SIRESP manual	

Figure 7. Indicator card for a sector-specific indicator at a lower CIRI level (here level 4), showing its parent indicators, context, description and measurement scale.

3.5 *Results from pilot implementation*

Based on the feedback from the initial demonstrations, ICI-REF was optimised, and the pilot implementation was conducted.

The resilience assessments resulted in suggestions for resilience treatment. Raising public awareness as well as training were pinpointed from the three tested methodologies. Application of CIRI resulted in recommendations to prevent silos, i.e. to have quick and easy cooperation between management and people in the field and to have structures in place to ensure this. Application of IORA actually identified that such a characteristic existed in the Barreiro organisation however more as an unofficial way of working. This demonstrates the ability of the different methodologies to bring up different levels of details and different perspectives.

The performance of ICI-REF in the pilot implementation is currently being critically evaluated with regards to the success factors. Generally, indicators were perceived by the operator as clearly described and easy to interpret, hence the adjustments made after the initial demonstrations had

improved ICI-REF significantly. When weighting the indicators, information from the operator could be valuable with regards to the importance of an indicator, but at the same time, it is important that the indicators are not biased towards the operator. The operator was of the opinion that ICI-REF can be valuable both as an internal audit tool and also in everyday work, and that it was useful in promoting reflection around resilience of the organisation and resilience treatment. The ability to compare results with other operators in the same sector outside of Portugal would also be useful for benchmarking purposes.

In order to provide an overall resilience score, all relevant indicators must be assessed. Although the pilot implementation assessed only a sample set of all the defined indicators, the operator found the results valuable for prioritising future work and development within their organisation.

4 DISCUSSION AND WAY FORWARD

After the initial demonstration of ICI-REF at the Barreiro living lab, the operator was of the opinion that indicators are crucial for monitoring resilience activities. However, to ensure that the assessment results are objective, consistent, repeatable, and representative of the assessed processes, the indicators should be defined using unambiguous terms. It was strongly suggested that clear questions should be asked for the operator to better understand what the indicator is assessing. The main potential for improvements of ICI-REF therefore lies in the design of sector-specific resilience indicators.

The indicators must not only be comprehensible and clear, but also at the same time leave some room for site-specific information. The degree of indicator specificity has been discussed with several living labs through the project, and the need for a balance between generality and specificity has been emphasised. If an indicator is too general, this may reduce the ability to detect details or new areas of resilience improvements. On the other hand, information about the specific CI can also be lost if the indicator is too detailed, which can make a further comparison with similar CI less relevant.

Regarding the measurement scales for the sector-specific indicators, it is not only challenging to define the scales, but it may also be challenging to assign quantitative value to a qualitative indicator without introducing subjectivity. The operator should therefore provide evidence and comments to support their assigned values for each indicator.

Despite the challenges in defining the indicator scales, weights and degree of specificity, the need for including sector-specific indicators are unquestionable. It should be described in terms of guidelines or references, at which level the indicators' scales and weights should be defined to ensure legitimacy. Benchmarked indicators exist within certain CI sectors. Although it may not be a requirement for a CI to compare to similar CI's, the living labs have expressed the wish to perform such a comparison at a regional level. However, for indicators that are not benchmarked, the comparison between similar CI will not be applicable if the operators, themselves, define scales and weights.

The indicator cards for the Barreiro living lab were successfully tested in the pilot implementation, as the indicators were considered well described and easy to assess and respond to. Indicator cards are now being developed for application in the next pilot implementation at another of the living labs in IMPROVER; the M1 highway in Budapest, Hungary.

5 CONCLUSION

The ICI-REF, technological and organisational resilience analysis methodologies and indicators have been applied and demonstrated in a pilot implementation, focusing on the potable water supply in Barreiro, Portugal. These have been developed with the aim to smoothly extend current risk management practices into a resilience management framework. A set of technological and organisational resilience indicators has been designed and described in "indicator cards". Efforts are made to improve the clarity of definitions and descriptions of resilience indicators, since unambiguous description of indicators is crucial for monitoring resilience activities. Based on the feedback from the Barreiro living lab during the project, initial demonstrations and a pilot implementation, the ICI-REF and the developed resilience analysis methodologies proved functional based on preliminary results.

They are now ready to be fine-tuned towards the next pilot implementation in IMPROVER. This focuses on the M1 highway in Budapest, Hungary, covers several scenarios and will be finalised in 2018. Combining results from the two pilot implementations allows evaluating the performance of the ICI-REF framework, methodologies and indicators to different CI sectors and contexts. Based on this, European guidelines for the resilience management to CI will be developed, addressed both to CI operators and policy makers.

ACKNOWLEDGEMENTS

Barreiro Municipality are acknowledged for valuable feedback and active participation in the

pilot implementation. This work is funded by the EU's Horizon 2020 research and innovation programme, grant agreement No 653390. It does not reflect the official opinion of the EU. Information and views expressed therein is the responsibility of the authors.

REFERENCES

Austr. Government (2017). Organisational Resilience Healthcheck; https://www.organisationalresilience.gov.au

Bram, S. et al. (2017) *Organisational resilience concepts applied to critical infrastructure*, IMPROVER Project: Deliverable 4.3.

Burgess, R.G. (1984) *In the Field: An Introduction to Field Research*, London: Allen and Unwin.

COM (2010) 673 final. *The EU Internal Security Strategy in Action: five steps towards a more secure Europe.* Brussels, 22.11.2010.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and assessment of the need to improve their protection.

Denzin, N.K. (1970). *The research act: A theoretical introduction to sociological methods.* Chicago: Aldine.

Denzin, N.K. and Lincoln, Y.S. (2011). *The Sage handbook of qualitative research*. Sage.

Hevner, A.R. et al. (2004). *Design Science in Information Systems Research*, MIS Quarterly, vol. 28, pp. 75–105.

ISO 22301:2012, *Societal security—Business continuity management systems—Requirements.*

ISO 22316:2017, *Security and resilience—Organizational resilience—Principles and attributes.*

ISO 31000:2009, *Risk management—Principles and guidelines.*

Kimchi, J. et al. (1991). *Triangulation: Operational definitions*. Nursing Research, 40(6), 364–366.

Lange, D. et al. (2017a). *Framework for implementation of resilience concepts to Critical Infrastructure, IMPROVER Project: Deliverable 5.1.*

Lange, D. et al. (2017b). *Incorporation of resilience assessment in Critical Infrastructure risk assessment frameworks*, In: Safety and Reliability—Theory and Applications, ISBN 978-1-138-62937-0, p. 1031–1038.

Mindykowski, P. et al. (2016). *Physical exposure identification and mapping methodologies*, IMPROVER Project: Deliverable 3.1.

Mitchell, E.S. (1986). *Multiple triangulation: A methodology for nursing science.* Advances in Nursing Science, 8(3), 18–26.

OECD (2011). *Future Global Shocks, Improving Risk Governance*. OECD Reviews of Risk Management Policies. ISBN 978-94-09520-5. 139 p.

Petersen, L. et al. (2018). *Creating comparable public tolerance and technical performance indicators for CI resilience.* ESREL 2018 (to appear).

Petit, F.D. et al. (2013). *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience.* ANL/DIS-13-01, Argonne National Laboratory, USA.

Pursiainen, C. et al. (2015). *Report of criteria for evaluating resilience*. IMPROVER Project: Deliverable 2.2.

Pursiainen, C.H. (2017) The Crisis Management Cycle. Routledge ISBN 9781138643871.

Resilient Organisations (2014). Resilience Benchmark Tool, New Zealand; available at http://brt.resorgs.org.nz

Rosenqvist, H. et al. (2018). *ISRA: A societal resilience analysis methodology*. ESREL 2018 (to appear).

Rossman, G.B. and Rallis, S.F. (2011). *Learning in the field: An introduction to qualitative research*. Sage.

SWD (2013) *318 final, Commission Staff Working Document a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure.* Brussels, 28.8.2013.

Theocharidou, M. et al. (2016). *Report of Operator Workshop 1*, IMPROVER Project: Deliverable 1.4.

UNISDR, United Nations Office for Disaster Risk Reduction, 2009 UNISDR terminology on disaster risk reduction; available at http://unisdr.org/.

Paper V

From risk management to resilience management in critical infrastructure

Rød, B., Lange, D., Theocharidou, M., and Pursiainen, C. (2020).

Published in *Journal of Management in Engineering,* 36(4): 04020039. DOI: 10.1061/(ASCE)ME.1943-5479.0000795.

Paper VI

Recoverability modelling of power distribution networks using accelerated life models: The case of power cut due to extreme weather events in Norway

Rød, B., Barabadi, A., and Naseri, M. (Forthcoming 2020).

Manuscript accepted for publication in *Journal of Management in Engineering*. DOI: 10.1061/(ASCE)ME.1943-5479.0000823.

Article published online on July 9, 2020. Printed version to be published in Volume 36 Issue 5 – September 2020

Recoverability modelling of power distribution systems using accelerated life models: The case of power cut due to extreme weather events in Norway

Authors: Bjarte Rød[1*], Abbas Barabadi[2], Masoud Naseri[3]

[1] M.Sc., UiT The Arctic University of Norway, Department of Technology and Safety, P.O. 6050 Langnes 9037 Tromsø, Norway, e-mail: bjarte.rod@uit.no

[2] Prof., UiT The Arctic University of Norway, Department of Technology and Safety, P.O. 6050 Langnes 9037 Tromsø, Norway, e-mail: abbas.b.abadi@uit.no

[3] Assoc. Prof., UiT The Arctic University of Norway, Department of Technology and Safety, P.O. 1063, 9480 Harstad, Norway, e-mail: masoud.naseri@uit.no

[*]Corresponding author: E-mail: bjarte.rod@uit.no, Tel: (+47) 98615331

ABSTRACT

Today's societies rely on electrical power distribution systems. Recent weather events have illustrated that the loss of such service can lead to severe consequences for societies and stakeholders. Hence, in order to reduce the impact of such extreme events on infrastructure systems and to limit the associated losses, it is crucial to design infrastructure that can bounce back and recover rapidly after disruptions (i.e. to be resilient). In this regard, it is vital to have knowledge of technical, organizational, internal, and external factors that influence the infrastructure's recovery process. These factors can broadly be categorized into two different groups, namely observed and unobserved risk factors. In most studies on resilience, the effect of unobserved covariates is neglected. This may lead to erroneous model selection for analyzing the time to recovery of the disrupted infrastructure, as well as wrong conclusions and thus decisions. The aim of this paper is to identify the risk factors (observed and unobserved) affecting the recovery process of disrupted infrastructure. To this aim, the paper extends the application of accelerated failure time (AFT) models, to model the recovery time of disrupted critical infrastructures in the presence of unobserved and observed risk factors. This model can be used to analyse how important these factors are from the viewpoint of resource allocation and decision-making. The application and implications of the model are presented in a case study, from both technical and management perspectives. The case study investigated in this paper applies the developed model, analysing recovery times from 73 disruption reports on Norwegian electric power distribution grids after four major extreme weather events. The analysis indicates that failures in the regional grid, natural conditions, area affected, and failures in operational control system have a significant impact on the recovery process.

Keywords: recovery, resilience, electric power distribution systems, critical infrastructure, extreme weather events, accelerated failure time models.

1 INTRODUCTION

Over recent decades, it has been evident that society relies heavily on infrastructure systems to provide and maintain vital societal functions (Rinaldi et al. 2001). Traditionally, in order to ensure the delivery of such functions, the focus of industry has been on the protection of the infrastructure systems from adverse and extreme events, such as hurricanes, tsunamis, floods, and so forth. However, recent events, such as Hurricane Sandy (Comes and Van de Walle 2014) and the tsunami that hit Japan in 2011, leading to a nuclear disaster (Bacon and Hobson 2014), illustrate that it is very difficult, and often not feasible, to protect such systems from all kinds of possible hazards. Hence, there has been a shift from the protection of critical infrastructure to the resilience of critical infrastructure, increasing the focus on preparedness, response and recovery (Pursiainen and Gattinesi 2014; Haimes 2012). In other words, having a resilient infrastructure, with the ability to limit the consequences of an impact through timely and efficient recovery processes, will certainly benefit the infrastructure operators and society as a whole (Choi et al., 2019). To effectively recover infrastructures from extreme events, it is essential for infrastructure operators to have knowledge of the factors (external, technical and organizational) that influence the recovery process. Such knowledge helps the analysts and decision-makers to make realistic estimates of the recovery rate and recovery time of the infrastructures.

Despite the growing number of studies on resilience in engineering systems, there is no common agreement as regards the definition of the concept or, more importantly, of how to assess and measure resilience (Hosseini et al. 2016). However, the most common resilience metric is the well-known resilience triangle, illustrating the loss of performance over time (Bruneau et al. 2003), as shown in Figure 1, adapted from Honfi et al. (2017). The figure illustrates the performance (Q) over time for a system experiencing some kind of incident, occurring at time t_i. The system develops a failure mechanism f. At time t_f, the system gradually starts to recover, through the process which is described by the recovery path r in Figure 1. At time t_r, the system is fully recovered and performs its required function at the same standard as before the incident.

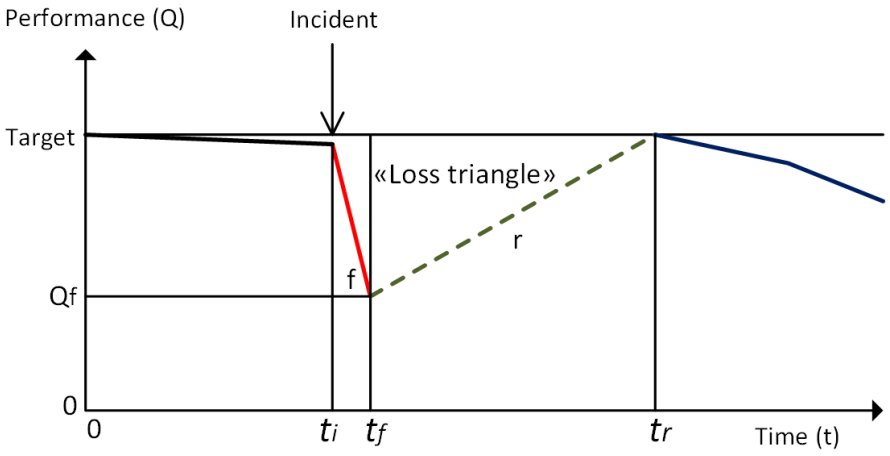

Figure 1. The performance loss function. Adapted from Honfi et al. (2017).

The resilience triangle illustrates the performance of the infrastructure over time, and, the smaller the triangle, the more resilient the infrastructure is. However, considering the trajectory of the recovery path and recovery time without investigating the environmental conditions and other conditions under which the recovery process takes place (i.e. influencing variables), such as number of crew, available resources, environmental conditions, region, technical condition of the system, etc., leads to a great deal of uncertainty and, thus, unreliable analysis results. A possible explanation for such results is that the recovery time as a random variable is, to a great extent, dependent on a set of prevailing operating or environmental conditions, which, through different mechanisms, can affect the length of the recovery time and, thus, recovery rate.

In general, having an effective contingency plan requires extensive knowledge concerning the recovery time of the specific system. Moreover, to have a reliable estimation of the recovery time, the effects of all factors that can influence the recovery process and path should be quantified, using appropriate models. Such models can be used as a basis for developing preparation plans, developing resource allocation strategies, identifying vulnerable recovery scenarios, and learning from the incidents. Influencing factors on the trajectory of the recovery path can be categorized into two groups: *i)* observed risk factors and *ii)* unobserved risk factors. Observed risk factors describe the recovery process characteristics (e.g. type of equipment used during the recovery process, number of maintenance personnel involved, etc.) or the environmental characteristics under which the recovery process took place (e.g. location of the disrupted infrastructures, cause of failures, weather conditions, etc.). Unobserved risk factors are independent variables that may have a significant impact on the recovery time of the infrastructure. However, these are not reported and thus not available in recovery databases. Observed and unobserved risk factors may lead to observed and unobserved heterogeneity. For example, in some situations, local people might help the repair crew to repair the failures and recover the infrastructure. However, their efforts and contribution to a reduced recovery time are not recorded in the corresponding databases. In this regard, their effect on recovery time should be modelled using unobserved risk factors.

Some methods, such as accelerated failure time (AFT) and proportional hazard (PH) models, have been widely used in order to analyse the effects of observed and unobserved risk factors, also known as covariates, on random duration time in survival analysis (e.g. Wei (1992); Bradburn et al. (2003); Orbe et al. (2002); Cox (2018); Fine and Gray (1999)). Although, in survival analysis, some studies have used PH and AFT models to analyse the impact of covariates on the hazard rate and survival time in various fields (e.g. Alvehag and Soder (2011); Alvehag and Soder (2008); Rocchetta et al. (2015); Tian et al. (2005); Peng and Huang (2007)), there is a gap in the literature, in which the application of such methods can be explored in the area of the recovery process of disrupted infrastructures and, in general, in resilience studies.

In this regard, the key novelty of the paper lies in exploring the application of AFT models in analysing the recoverability of disrupted infrastructures, in addition to analysing the impact of observed and unobserved risk factors on the recovery time. This is achieved by considering the operating conditions and other covariates, where the recovery time is selected to be the random variable of interest. Therefore, the results of this study enable managers to make informed decisions regarding resource allocation,

contingency plans, and preparedness plans. From a managerial perspective, the response and recovery process can be optimized by taking these factors into consideration. In so doing, the consequences for the customer and society will also be reduced.

Although the presented approach in the current study can be used in various critical infrastructures, the scope of the present case study is electric power distribution systems. The case study is resolved by analysing the recovery times from outages corresponding to 73 disruptions within the Norwegian system from 2013 to 2016, after four extreme weather events. Therefore, the method is illustrated by a case that consists of major parts of the electric power distribution and transmission grid in Norway. The main driver for choosing electric power distribution as the case study is the fact that it is among the most important critical infrastructures. Considering the high level of interdependency between critical infrastructures in our modern societies (e.g., transportation, health, power distribution, communication, water supply, etc.), any disruption in electric power distribution can trigger the disruption of other mentioned infrastructures. Hence, all electric power distribution companies should have clear understanding regarding the recoverability, i.e. the ability of the organization to recover from disruptions, of their power distribution systems. Moreover, it is crucial for the operator to know how to optimize the recovery process with limited resources in place. Normally, these companies apply relatively simple deterministic models, based on damage assessment in the field, to estimate recovery time, which can only be applied after the event has occurred. Such models are not able to identify the significance of the (observed and unobserved) risk factors and the extent of their impact. Considering the importance of power distribution systems for our society, there is an urgent need to develop some new statistical approaches for modelling the effect of observed and unobserved risk factors on their recoverability. To this aim, the contribution of this paper goes further in employing the AFT model to identify important parameters affecting the recovery of Norwegian electric power distribution systems and in analysing how important these factors are regarding resource allocation and decision-making in future disruptions of the power distribution grid. In addition, this study gives guidance on the use of suitable statistical models for generating accurate and reliable results, which can provide infrastructure operators with valuable information when making important decisions before, during and after a disruption.

The rest of the paper is organized as follows. First, a general discussion about resilience is presented, followed by a literature review about prediction and modelling of resilience and recovery. Thereafter, the Norwegian electric power distribution system is described. The data and methodology are then described, and results from the case study are presented. Finally, some conclusions and recommendations for future works are provided.

2 BACKGROUND AND LITERATURE REVIEW

2.1 Resilience definition and metrics

The definition of resilience is a contested one, and there is no clear definition of the concept, at this time, that could be applied universally (Rochas et al. 2015). The original meaning of the word comes from the

Latin word *resilire*, which can be understood as the "ability to rebound or jump-back" (Dalziell and McManus 2004), highlighting the essence of the concept – the ability to bounce back. In material science, resilience is understood as the ability of materials to recover their shape after being stretched or deformed (Dessavre et al. 2016). In the context of disaster risk reduction, the United Nations (UNISDR n.d.) provides a comprehensive and general description of resilience, as follows: "*the ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management"*. This definition emphasises that resilience has its temporal dimensions, including the ability to resist. From a social perspective, Cutter et al. (2008) describe social resilience as *"the ability of a social system to respond and recover from disasters that includes those inherent conditions that allow the system to absorb impacts and cope with an event, as well as adaptive processes that facilitate the ability of the social system to reorganize, change and learn in response to a threat"*. It can be argued that, to some extent, adaptive and absorptive capacities are developed prior to the event, implying that the pre-event stage is also included here. This implies that resilience is, as stated by Lange et al. (2017a), "*a process that has to be present and enhanced before, during and after a crisis or disruption of services"*. Nevertheless, the exact effect of measures implemented before a crisis is only known after the event.

From an engineering and technical point of view, the key elements related to resilience consist of concepts such as resistance, absorption, adaption and recovery (Francis and Bekera 2014). In many ways, resilience integrates, for better or worse, existing measures of risk, vulnerability, reliability, robustness, survivability, adaptability, maintainability, availability, and so forth, in order to measure resilience (Faturechi and Miller-Hooks 2014). Hence, how one measures and quantifies resilience will, of course, depend on the concept(s) one includes and the metrics and units that are applied to measure these concepts. In essence, this relates to the drop or loss in performance (as described in Figure 1), as a direct or indirect consequence of an abnormal situation. Bollinger and Dijkema (2016) measure this loss in performance in terms of service level, evaluating the resilience level of the Dutch electricity transmission network as a mean fraction of demand served across the range of possible extreme event magnitudes. Cimellaro et al. (2014) measure the infrastructure service level after the 2011 Tohoku earthquake in Japan as the restoration ratio between the number of households without service and the total number of households. Hossain et al. (2019) emphasise that "*Resilience is the ratio of recovery"*, measured as recovered production capacity to lost production capacity. Other studies focus more on the functional level of the infrastructure systems. For instance, Ouyang et al. (2012) state that "*The performance level is measured by the number of normally operating components within an infrastructure system*". Similarly, Rochas et al. (2015) use the total length of functioning pipelines as a 'figure of merit' to measure the functional level of an infrastructure. There are also studies that focus on the general quality of the infrastructure systems, such as Mendonça and Wallace (2006), who investigated the number of disruptions for each infrastructure during various weeks of the event, in order to analyse the impacts of the World Trade Centre attack in New York on city critical infrastructures over a three-month period.

For this case study, resilience will be defined in accordance with the time to recovery, where the resilience metric is the service level, measured in terms of end users with power supply. Hence, based on this definition, the AFT model is used to model the time to recovery, considering the effect of observed and unobserved risk factors. It should be mentioned that the recoverability will be modelled by the number of customers affected by the disruption. A limitation of this metric is that the occurrence of disruptions in less populated areas may not reflect the magnitude of the disruption and the level of physical damage. However, in many quantitative resilience assessment methodologies, the recoverability or recovery rate is considered only as a minor part of the resilience definitions (the other parts are prevention, absorption, adaptation) (see e.g. Francis and Bakera (2014) and McEvoy et al. (2012)). However, the weight placed on the recovery phase, compared to other phases of resilience, may vary, based on the selected definition. For example, in the engineering and technical area, where resilience is often divided into several phases and described by several concepts, such as resistance, absorption, adaption and recovery (see e.g. Ouyang & Wang (2015); Kong et al. (2019)), the developed model in this study would then be a part of a more comprehensible definition of resilience. In other words, regardless of the definition of resilience, the recovery is always an important phase, and the model presented in this study is thus applicable in the resilience context.

2.2 Prediction and modelling of resilience and recovery

In general, as stated by Hosseini et al. (2016), quantitative resilience assessment methodologies can be divided into general measures and structurally based models. General measures include probabilistic and deterministic measures, while structurally based models include optimisation, simulation and fuzzy logic approaches. Modelling and simulation of critical infrastructures has become a key field of study, and numerous approaches have been developed over recent years (see studies such as Ouyang (2014) and Hosseini et al. (2016)). A common feature of such models is that they investigate how the structure of the system impacts the resilience level. This is done by observing the system behaviour and modelling and simulating the characteristics of the system. Many of these models represent a real-life restoration process, including a high level of detail (e.g. Çağnan et al. (2006)), which requires a huge amount of data to be being collected and processed.

Probabilistic approaches, categorised as general measures, account for uncertainty, and the stochastic behaviour of the disruptive events, as well as the stochastic behaviour and randomness of duration (i.e. recovery time), are, to a large extent, captured. For instance, Youn et al. (2011) describe resilience by using two traditional concepts, namely, reliability and restoration, where restoration is described as the joint probability of a system failure event, a correct diagnosis event, and a mitigation/recovery action success event. Restoration and recoverability is often referred to as maintainability in conventional reliability engineering, defined as "*the ability of an item under a given condition of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources*" (International Electrotechnical Vocabulary (IEV) 191 2007). In maintainability analysis methods, the repair or restoration time is considered a random variable (Blanchard et al. 1995, Dhillon 1999). The aim of such

analysis methods is to model the probability that a successful repair process takes place within a stated time interval under procedures and resources (Barabadi et al. 2011), also known as survival analysis. Qiao et al. (2019) classify survival models as non-parametric, semiparametric, or fully parametric. The nonparametric can be easily implemented and does not require any assumptions. However, as stated by the definition of maintainability, the time required for restoration or repair depends on a range of conditions under which the restoration process occurs. Such conditions may include technical features, organisational aspects, and environmental conditions. The nonparametric models do not have the ability to relate these external factors to the restoration function. In order to capture the impact of these conditions and elements, also known as influencing variables or covariates, fully parametric models can be used. AFT and PH models are often used (e.g. Barabadi et al. (2011); Kayrbekova et al. (2011); Naseri (2017)) to study the extent to which the repair time or maintainability depends on the underlying conditions. In an analogy with the maintainability analysis, one may focus on the application of AFT and PH models in the recoverability of an infrastructure unit after a disruptive event. Such models provide the analysts with an opportunity to analyse the impact of different influencing parameters on recovery time or, in general, on recoverability. In this regard, recoverability can be defined as the ability of an organisation to restore an infrastructure unit to a level that is able to deliver required functions as before the occurrence of the disruptive event.

The study by Liu et al. (2007) was one of the first to implement survival analysis to model power outage restoration times during hurricanes and ice storms, using AFT and Cox proportional hazard (Cox PH) models. The authors conclude that AFT is better than Cox, mainly because the results from AFT are easier to interpret. Nateghi et al. (2011) compare five statistical models for estimating power outage duration times: AFT, Cox PH, and data mining techniques (regression trees, Bayesian additive regression tree (BART), and multivariate additive regression splines). They state that BART yields the best predication accuracy but emphasise that the AFT model "*provides a further basis for examining the influence of each covariate on the restoration periods*". Similar statistical methods have been applied in a variety of fields and disciplines, such as health science (e.g. Bakhshi et al. (2017)), accident investigations (e.g. Saeed et al. (2019a and b)), project management (e.g. Qiao et al. (2019)), and the oil and gas industry (e.g. Ilbeigi & Dilkina (2017)) – underlining the broad application area of such methods. However, as mentioned in the introductory section, these studies do not consider the effect of unobserved risk factors. In general, due to the nature of the recovery process, recovery procedures, location of the accident, type of accident, culture of the people affected by the disrupted infrastructures and so on, it is very difficult to capture and record all risk factors in the recovery database. Moreover, our experience with the Norwegian electric power distribution systems and oil and gas industries can confirm this fact: that most of the available recovery data are not very well collected and they do not reflect the actual environmental conditions of the recovery site of the infrastructure. Considering the fact that the results of the recovery analysis will be used later for learning processes in contingency planning, neglecting the impact of unobserved risk factors would lead to biased results and thus unrealistic resource distribution and planning.

2.3 The Norwegian Electrical Power Distribution System

The Norwegian electric power distribution system is divided into three different levels, namely, the distribution grid, the regional grid, and the transmission grid. Consistent with international terminology, we in this paper often use 'distribution grid' as an umbrella term for both the distribution and the regional grid in Norway. The transmission grid, has the highest voltage level, ranging from 132 kV to 400 kV; it acts as a link between the producers and the customers in a nationwide system. The transmission grid is about 11,000 km. It is mainly operated by Statnett SF, which is the only Transmission System Operator (TSA) owned by the state; licensed by the Norwegian Water Resources and Energy Directorate (NVE), it is regulated by the Norwegian Energy Act of 1990. The regional grid is the link between the transmission grid and the distribution grid. However, some parts of the grid also consist of production and consumption radials. In total, the regional grid is 19,000 km, of which 8% comprises sea and underground cables. The distribution grid serves the end user, such as households, public services, and industry, with power. The voltage level ranges from 22 kV to 230 V. In total, the distribution grid consists of 100,000 km of lines with a voltage level above 1 kV, of which 40% comprises sea and underground cables (Hatlen and Knudsen Aarrestad 2015).

The Norwegian Water Resources and Energy Directorate (NVE), organised under the Norwegian Ministry of Petroleum and Energy, has the overall responsibility for maintaining the national power supply. One of the directorate's tasks is to issue regulations on system responsibility and to ensure the quality of the power supply. All Norwegian grid companies are obliged to report interruptions to NVE. In 2015, a total of 159 companies operated in the Norwegian electric power grid on one or several levels. These 159 companies cover different geographical areas in Norway, and there is a large deviation among the companies in terms of the number of customers served, size of the service area, geographical characteristics, and so forth. Each company is regulated under the 'compensation for non-delivery of energy' (KILE). This gives distribution companies reduced income in the event of an interruption. As stated by the Norwegian government, "*The KILE scheme is a means for distribution companies to be confronted with customer interruptions cost and take into consideration these costs when making decisions*". This KILE scheme thus ensures that reliability is taken into account when the companies make important decisions, both during operation and with respect to future investments.

In the case of interruptions in the power supply, and to ensure the quality of the supply, each company is obliged to report failure data to the regulator, which is NVE. This is done through the Fault and Supply Interruption information Tool (FASIT), developed in the 1990s. Since 1995, all Norwegian grid operator companies are required to use this tool for the collection and reporting of component fault and delivery point interruption data (Heggset et al. 2009). In addition, when extreme weather events occur, such as major autumn and winter storms, each company that is affected by the storm must prepare and submit extensive reports to NVE. Such a report includes a range of qualitative and quantitative data. The qualitative data concerns the operator's subjective opinions on how the organisation managed to prevent or recover from disruption and power cut. Such data is a valuable source of information that gives a much clearer picture of the recovery process, integrating the organisational and technical resilience domains.

3 DATA AND METHODOLOGY

In this case study, considering the available data, the AFT model is applied. As emphasised in the literature review, there exists a wide range simulation and modelling approaches applicable for infrastructure systems. However, without detailed information about the system characteristics, such methods might produce inaccurate results.

3.1 Model

In risk and reliability analysis fields, the time to failure of a system or the time to repair a failed component is considered a random variable (Rausand and Høyland 2004). This can also be applied to analysing the resilience of infrastructures, including power distribution grids, where the time that it takes to have the grid in the new equilibrium state or back to its normal operating level can also be considered a random variable (Francis and Bekera 2014, Hosseini et al. 2016). The randomness of the time to recover a power distribution grid thus requires the application of probabilistic models.

More specifically, in the current modelling setting, the variable of interest is the duration or the length of time that the recovery process takes. This parameter, which is inherently a random variable, is often referred to as recovery time, as shown by the length $t_f - t_r$ in Figure 1. Such a time interval begins with the initiation of recovery efforts, which is usually upon noticing the power outage, until the recovery process is finished and electricity is again provided for customers.

Let T be a positive random variable, denoting the recovery time. Also, let $f(t)$ be the corresponding probability density function (pdf) of random variable T. Thus, the cumulative distribution function (cdf), $F(t)$ of random variable T (Rausand and Høyland 2004) – which, in the current modelling framework is recoverability denoted by $R(t)$ – expresses the probability that the recovery process is completed at time $T < t$. Therefore, the recoverability can be defined by Equation (1):

$$R(t) = \Pr(T < t) = \int_0^t f(u)du \tag{1}$$

Using such terminology, the recovery rate, denoted by $r(t)$, is defined as the probability that the recovery is completed in the time interval $(t, t + \Delta t]$ when it is known that the recovery has not been completed until time t (i.e., it is known that electricity is still down at time t and customers experience a power cut at time t):

$$r(t) = \Pr(t < T \leq t + \Delta t | T > t) = \frac{\Pr(t<T\leq t+\Delta t)}{\Pr(T>t)} = \frac{f(t)}{1-R(t)} \tag{2}$$

By combining Equations (1) and (2), the recoverability function, $R(t)$, can be expressed as:

$$R(t) = 1 - \exp\left[-\int_0^t r(u)du\right] \tag{3}$$

Survival function, $S(t)$, is another important concept in duration analysis, given as (Rausand and Høyland 2004):

$$S(t) = \Pr(T \geq t) = 1 - \int_0^t f(u)du$$

In the context of the present study, $S(t)$ states the probability that the recovery cannot be completed before some specified time t:

$$S(t) = 1 - \int_0^t f(u)du = 1 - F(t) = \exp\left[-\int_0^t r(u)du\right] \quad (4)$$

However, Equations (1) to (4) do not include the impact of any covariate or operating condition on the recoverability or the recovery time of the power grid. In survival analysis, various models including accelerated failure time (AFT) and proportional hazard (PH) models have been widely used, in order to analyse the effects of explanatory variables (also known as covariates) on the random duration time (e.g. Wei (1992); Bradburn et al. (2003); Orbe et al. (2002); Cox (2018); Fine and Gray (1999)). The main difference between the AFT and PH models lies in modelling the impact of covariates on the random dependent variable, i.e. duration of recovery time. While, in AFT models, covariates have multiplicative effects on time, in PH models, covariates have multiplicative effects on hazard rate (Kumar and Klefsjö 1994, Nelson 2009). Such models have also been widely used in reliability, availability, and maintainability analyses, in order to capture the impact of covariates on failure and repair times (see e.g. Bagdonavicius and Nikulin (2001); Ghodrati and Kumar (2005b); Crowder (2017); Naseri and Barabady (2016); Naseri et al. (2016)). Different types of covariates are used in such studies including environmental conditions (Barabadi 2014), weather conditions (Naseri et al. 2016), and skill level of operation crew (Ghodrati and Kumar 2005), as well as location of the plant and batch of the production, as discussed in studies by Ansell and Philipps (1997); Dale (1985), Jardine et al. (1987) and Kumar et al. (1992).

Given the above-mentioned discussion, and due to the fact that the the recoverability of an infrastructure unit and its recovery rate after the occurrence of a disruption depend on a number of parameters and conditions under which the recovery process takes place, the current study employs the AFT model to investigate the impact of the influencing parameters (i.e., operating and environmental conditions) on the recovery time of power grids after disruption.

As mentioned earlier, in AFT models, the effects of covariates or explanatory variables on the random variable time are expressed as multiplicative factors to the time (Bagdonavicius and Nikulin 2001, Kumar and Klefsjö 1994, Nelson 2009). In other words, according to the general log-linear relationship between time T and a vector of covariates, the natural logarithm of recovery time is expressed as a linear model of the covariates (Nelson 2009), as given by Equation (5):

$$\ln T = \alpha_0 + \sum_{k=1}^{n} \alpha_k x_k \quad (5)$$

where n is the total number of covariates, $x_k, k = 1, \dots n$ is the kth covariate, $\alpha_k, k = 1, \dots n$ is the regression coefficient, and α_0 is a constant error term. The distributional form of the error term determines the regression model. Various distributions can be used to develop the recovery time model, including Weibull, exponential, and lognormal (Lee and Wang 2003, Rausand and Høyland 2004).

Due to the flexibility of the Weibull distribution in modelling different patterns of hazard rates, this study uses the Weibull distribution as the underlying distribution model, which has a probability density function given by:

$$f(t) = \frac{\beta}{\eta^\beta} \mathrm{t}^{\beta-1} 1 - \mathrm{e}^{-\left(\frac{t}{\eta}\right)^\beta} \quad (6)$$

where η and β are the scale and shape parameters. The recoverability function can then be obtained by substituting Equation (6) into Equation (1):

$$R(t) = 1 - \mathrm{e}^{-\left(\frac{t}{\eta}\right)^{\beta}} \quad (7)$$

According to the approach suggested by the Department of Defence (1991), in AFT models, the independent random time variable is modelled by multiplying the baseline time, say t_0, by a functional form, $\exp(\alpha_k x_k + \alpha_k x_k + \cdots + \alpha_k x_k), k = 1, \ldots, n$, which represents the impact of covariates on the independent variable, time. Thus

$$t = \exp(\alpha_k x_k + \alpha_k x_k + \cdots + \alpha_k x_k)\, t_0 \quad (8)$$

where t_0 is the recovery time under base conditions. By substituting Equation (8) into Equation (7) and according to the equivalent age concept (Naseri et al. (2016), Department of Defence (1991), the recoverability function under the impact of covariates can be rewritten as:

$$R(t|x_k) = 1 - \mathrm{e}^{-\left(\frac{t}{\eta \exp(\alpha_k x_k + \alpha_k x_k + \cdots + \alpha_k x_k)}\right)^{\beta}} \quad (9)$$

or

$$R(t|x_k) = 1 - \mathrm{e}^{-\left(\frac{t}{\exp(\boldsymbol{AX})}\right)^{\beta}} \rightarrow R(t|x_k) = 1 - \exp\left[-t^{\beta} \exp[-\beta \boldsymbol{AX}]\right] \quad (10)$$

where β is the shape parameter of the Weibull distribution, $\boldsymbol{A}$ is the regression coefficient row vector including the constant error term, $\alpha_k, k = 0, \ldots n$, where $\alpha_0 = \ln \eta_0$ and $\boldsymbol{X}$ is the covariate column vector with $x_k, k = 0, \ldots n$, where $x_0 = 1$ and η_0 is the scale parameter under base conditions.

Equation (10) can be used to express the impact of covariates or environmental conditions on the recoverability of the power grid. By substituting Equation (10) into Equation (3), the recovery rate under the influence of covariates can be obtained:

$$r(t|x_k) = \beta t^{\beta} \exp[-\beta \boldsymbol{AX}] \quad (11)$$

In Equations (10) and (11), covariates $x_k, k = 1, \ldots n$, can be dependent or independent of time. In other words, the corresponding values of these covariates either change with time or can be assumed to be constant. In the present study, it can be assumed that these covariates do not change within the time frame of recovery. In other words, the covariates $x_k, k = 1, \ldots n$ are assumed to be time-independent. Regression coefficients are estimated using maximum likelihood estimation methods (Lee and Wang 2003, Neath and Cavanaugh 2012, Pan 2001, Volinsky and Raftery 2000).

Traditionally, AFT and PH models are used with the assumption of homogeneity of the cumulative distribution function across the individuals (i.e. observations). However, this assumption leads to a great deal of uncertainty – if not wrong results – if some heterogeneity is present among the observations. Moreover, traditional analyses assume that the observations are independent (Hougaard 2016, Mohammadian and Doherty 2006, Yashin et al. 1995). However, in the context of the current study, it can be argued that, in certain cases, some failed components of the system are repaired, and the electricity power grid is brought back to operation so that a group of customers receives electricity. This indicates a group recovery for some power cut scenarios, i.e. electricity is provided for a group of customers, by repairing certain failed components.

Given the above discussion, one should account for the unobserved heterogeneity in the observation; different approaches are used for this in the literature. Some researchers have used random parameter models (Seraneeprkarn et al. 2017; Rahman Shaon et al. 2018; Afghari et al. 2019; Saeed et al. 2019) in estimating car crashes and the impact of some explanatory variables on the number of crashes in a road segment. In such studies, the coefficients of the covariates are assumed to be random variables. This implies that the coefficients have different effects on different observations. In other words, the heterogeneity of the explanatory variables is estimated through the randomness of coefficients. Some justifications for choosing random regression coefficients and thus using random parameter models is provided in a study by Mannering et al. (2016), where the random effect of different variables, including human elements, vehicle characteristics, safety-feature indicators, as well as roadway and traffic characteristics, on the number of road car crashes is discussed. Another approach, which is used in duration analysis and is employed in the current study, relies on shared frailty models, where the effect of heterogeneity is modelled by introducing a multiplicative parameter, known as shared frailty, to the hazard function (Yue and Chan 1997; Hougaard 1995; Matsuoka 2010; Hanagal 2017; Nath et al. 2016; Hesam et al. 2018; Fagbamigme et al. 2019). This also accounts for the presence of unobserved covariates that affect the recovery rate and recoverability. Shared frailty is, in fact, a group-specific unobserved or latent random effect, which is multiplied by the recovery rate function. Another role of shared frailty in the recoverability model is to generate some dependency among the observations that can be grouped together (Gutierrez 2002).

In order to account for the shared frailty, let the data consist of M groups, with one of them consisting of N_i individuals. The frailty of the ith group is then denoted by ε_i, which is a positive random number with mean equal to 1, variance θ, and the probability density function $g(\varepsilon_i)$. Those individuals or observations with $\varepsilon_i > 1$ are said to be frailer, for reasons left unexplained by the observed covariates, and will experience a higher recovery rate. Conversely, those individuals or observations with $\varepsilon_i < 1$ are less frail and will tend to have a lower recovery rate. Observations with higher and lower recovery rates tend to be associated with lower and higher recovery times, respectively. By introducing the frailty parameter, the conditional recovery rate and recoverability function for individual j in the ith group can be written as in Equations (12) and (13), respectively (Gutierrez 2002, Hougaard 1995, Wienke 2010):

$$r_{ij}(t|\varepsilon_i) = \varepsilon_i h_{ij}(t) \tag{12}$$

$$R_{ij}(t|\varepsilon_i) = 1 - \exp\left[-\int_0^t \varepsilon_i r_{ij}(u)du\right] = 1 - \left[S_{ij}(t)\right]^{\varepsilon_i} \tag{13}$$

where $j = 1, \dots, N_i$, $i = 1, \dots M$, $h_{ij}(u)$ and $F_{ij}(t)$ are individual non-frailty recovery rate and recoverability functions, respectively. The unconditional survival function and unconditional recoverability function for individual j in the ith group, when the frailty is present, are then obtained using Equation (13) and are given by Equations (14) and (15), respectively (Gutierrez 2002, Hougaard 1995, Wienke 2010):

$$R'_{ij}(t) = \int_0^\infty g(\varepsilon_i)R_{ij}(t|\varepsilon_i)d\varepsilon_i = \int_0^\infty g(\varepsilon_i)\left[1 - \left[S_{ij}(t)\right]^{\varepsilon_i}\right]d\varepsilon_i \tag{14}$$

$$S'_{ij}(t) = 1 - \int_0^\infty g(\varepsilon_i)R_{ij}(t|\varepsilon_i)d\varepsilon_i = \int_0^\infty g(\varepsilon_i)\left[S_{ij}(t)\right]^{\varepsilon_i}d\varepsilon_i \tag{15}$$

Gamma distribution is a common distribution model for handling the heterogeneity of the data. By assuming a gamma-distributed shared frailty, given by Equation (16) (Gutierrez 2002, Hougaard 1995, Wienke 2010):

$$g(\varepsilon_i) = \frac{{\varepsilon_i}^{1/\theta-1}\exp(-\varepsilon_i/\theta)}{\Gamma(1/\theta)\theta^{1/\theta}} \tag{16}$$

The unconditional survival function and unconditional recoverability function for individual j in the ith group, when the frailty is present, can be written as (Gutierrez 2002, Hougaard 1995, Wienke 2010):

$$R'_{ij}(t) = 1 - \left[1 - \theta \ln\left[1 - R_{ij}(t)\right]\right]^{-\frac{1}{\theta}} \tag{17}$$

By also introducing the observed covariates, Equation (13) can be rewritten as:

$$R_{ij}\left(t|\varepsilon_i, x_k^{ij}\right) = 1 - \exp\left[-\int_0^t \varepsilon_i r_{ij}\left(u|x_k^{ij}\right)du\right] = 1 - \left[S_{ij}\left(t|x_k^{ij}\right)\right]^{\varepsilon_i} \tag{18}$$

where $x_k^{ij}, k = 1, \dots, n$ is the kth covariate of individual j in the ith group. By assuming a gamma-distributed frailty, the unconditional form of Equation (18) can be written as:

$$F'_{ij}\left(t|x_k^{ij}\right) = 1 - \left[1 - \theta \ln\left[1 - F_{ij}\left(t|x_k^{ij}\right)\right]\right]^{-\frac{1}{\theta}} \tag{19}$$

where $R_{ij}\left(t|x_k^{ij}\right)$ can be obtained using Equation (10) for a Weibull distribution model.

3.2 Data collection and extraction

In this case study, data are extracted and analysed from 73 interruption reports from electric power distribution companies, reported from 2013 to 2016, after four extreme weather events, namely "Hilde", "Ivar", "Tor", and "Nina". This data is partly sensitive, and the reports are not publicly available. Through an agreement with the regulator, the authors of this study were granted access to data from six extreme weather events. However, due to inconsistency in the reporting procedure, only four of the events were selected for further analysis. Moreover, the four weather events selected have quite similar characteristics, which is believed to be an advantage when comparing the recovery processes. The four events are described below.

- *Hilde:* 'Hilde' took place on January 16-17, 2013, with wind speed corresponding to violent storm, and with hurricane force for shorter periods, affecting the area between Trondheim and Bodø. The strength of the weather peaked in the evening and, at 3 am, on January 17, the extreme weather situation was considered over. Approximately 83,000 end users experienced interruptions during the event, while 27,674 customers had their power supply recovered within one hour. The total economic consequence of the event, including KILE costs, was estimated at NOK 51 million. In total, around 400 persons were involved in the short-term recovery process. Only four grid operator companies were affected by this event. However, it should be noted that these companies cover large areas of Norway.
- *Ivar:* The extreme weather 'Ivar' struck middle parts of Norway in the afternoon of December 12, 2013. A low pressure moved in from Great Britain and hit Trøndelag County and Møre og Romsdal County, with wind speed corresponding to violent storm and hurricane. The extreme period of the

weather lasted for a relatively short period, ending after six hours at 9 pm in the evening. Approximately 110,000 end users were affected by the weather, of which 81,000 experienced interruptions of over one hour, and 29,000 had an outage lasting for more than 12 hours. The total economic consequence was estimated at NOK 93 million, and around 630 persons were involved in the short-term recovery process.

- *Tor:* This weather event took place on January 29, 2016. It moved in from the North Sea and first hit the southern parts of Norway and then moved northward to Nordland County. A wind of hurricane strength was measured in several places, with a maximum speed of 48.9 m/s. The severity of the weather declined during the night and, from the morning of January 30, the wind strength was no longer characterised as extreme. Approximately 180,000 outages were registered, of which only 1000 were longer than 24 hours. In total, 150,000 customers were affected by interruptions over the course of the event, some of which experienced several outages. The total damage caused by the event was estimated at NOK 41 million, and more than 800 persons were involved in the short-term recovery. A total of 37 grid companies were affected by this event.
- *Nina:* The extreme weather event 'Nina' struck south-western parts of Norway on January 10, 2015. According to The Norwegian Meteorological Institute (MET) (2015), Nina was one of the five strongest storms registered in Norway during the last 60-70 years. The storm affected large parts of southern Norway, including the urban areas around Oslo. The extreme period of the weather lasted for almost 12 hours. In total, 250,000 end users experienced interruptions during the event, of which 40% had their power supply recovered within one hour, while over 100,000 end users were without power for more than 12 hours. The total damage caused by the event was estimated at NOK 175 million, while 927 persons were involved in the short-term recovery process.

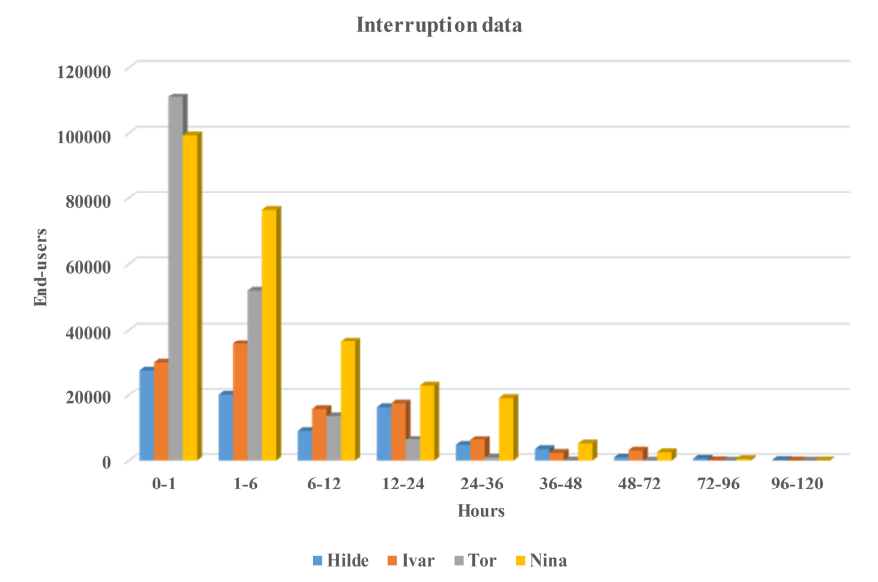

Figure 2. Chart showing number of outages in given time intervals for four different extreme weather events.

As discussed, in the case of interruption in the distribution companies' grids, they are obliged to report this in the FASIT-system. Moreover, each grid company affected by an extreme event, such as the events described above, is committed to deliver written reports to NVE. The data set used in this case study is based on such reports, and a brief description of the content of these reports is provided in the next paragraph. A summary of the reported data is found in Table 1.

Table 1. Summary of reported data.

Report metric	**Sub-categories/metric**	**Description**
County		19 Norwegian counties
Time and date		Time and date of impact
Place	City, urban and rural	Description of place (more than one is possible)
Natural conditions causing failures	Lightning, precipitation/flooding, Vegetation/trees, wind, salting, avalanche, pollution, fire, birds/animals	Qualitative description of the natural conditions that caused failures
Technical failures	Wear, mechanical failure, heat, electrical failure, fatigue, corrosion	Qualitative description of the types of technical failures
Number of persons involved in the recovery process	Internal employees, external entrepreneurs, landowners, other resources	Operators points out the number of persons involved in the recovery process, divided in four categories.
Costs	Production loss, material costs, KILE-costs, labor costs, compensation costs, other.	Operator estimate the cost out the outages caused by the storm, divided in six categories.
Damage in the grid	Transmission grid , regional grid, distribution grid	Operator states which objects in the grid that is affected, and at which voltage level.
Stations affected	Transmission grid , regional grid, distribution grid	Operator states stations that are damaged (transformation station or connecting station),
Customers without power supply	0-1 hrs., 1-6 hrs., 6-12 hrs., 12-24 hrs., 24-36 hrs., 36- 48 hrs., 2-3 days, 3-4 days, ...7-8 days.	Number of customers without power supply reported in time intervals

The first section of the report includes a general description of the event. This includes information about the time of impact, which could have an effect on the length of the recovery time, e.g. if it is at night, during holidays, on weekdays or weekends. In addition, the companies describe the areas affected, whether city, urban area, and/or countryside. Furthermore, the operator specifies the cause of the disruption, distinguishing between natural causes and technical causes/failures. Next, the total number of employees (not man-hours) involved in the recovery process is reported. The same information is given with regard to external personnel. Moreover, the companies can report what other resources they have had access to, such as boats, helicopters and excavators.

The next section in the report deals with the economic consequences of the event. The companies provide estimates for associated costs, divided into several categories. Then, the companies highlight the affected objects in the system, differentiating between different parts of the system, such as voltage level. The companies are also required to state the number of failures that have occurred in each subsystem.

However, the exact number of failures is often missing and, if provided, is usually limited to the total number of failures in the system as a whole. In the last part of the report, the companies report whether they have experienced failures relating to other objects, such as their operational control system and operational centres.

At the end of the quantitative part of the report, the companies provide detailed interruption data in terms of the number of outages in certain intervals, where one outage equates to one end user without power for a given time. The outages are not reported in chronological order, and it should also be noted that the same customers may experience more than one outage during one event, i.e. the sum of the number of outages does not necessarily represent the total number of customers affected. Figure 2 compares these four events by illustrating the interruption data for each event in terms of number of outages.

The last part of the report consists of a set of questions, wherein the operators can carry out some qualitative evaluations. Some key aspects here are how they experienced the communication process during the event (both internal and external), the role of exercises, their assessment of the recovery process, condition monitoring and forest clearance, and the effect of the operational control system in the recovery process.

3.3 Variables for analysis

Table 2 shows the list of covariates and their values used in this study. Due to the quality of the reported data and the limited number of data points (n=73), a few key variables are selected to be included in the analysis. Many of the reports contained incomplete data, and, hence, some report metrics in the reports was excluded for the analysis. The selection of variables was based on a literature review and recommendations from the regulator (NVE).

The variable *Event* is a categorical variable that denotes the extreme weather event that has caused the outages. *Location* is a categorical variable, denoting the location of the affected area. *County* is a categorical variable, which lists the counties of Norway and represents the county wherein the extreme event and, thus, the outage has occurred and been reported. *NaturalCondition* is a categorical variable that represents the natural conditions causing the failures and interruption in the power supply. *FailureRegNet* is a logical variable, describing whether the companies have experienced failures in higher voltage levels or in the regional grid or not (i.e. Yes/No). *FailureStation* is a logical variable, stating whether the companies had failures in stations, which could be both transforming stations and connecting stations, independent of voltage level. *CommunicationQuality* is a categorical variable that represents the quality of communication among the actors and personnel during the recovery process, categorised on three levels: poor, sufficient and good. *FailureControlSystem* is a logical variable, stating whether the companies have experienced any complications in their operation control system, which is an essential system used to localise failure and to reroute power supply. *Exercises* is a logical variable that refers to whether the companies have performed exercises based on similar scenarios. *TreeFallPercent* is a continuous numerical variable, assigned by the operator, that denotes what percentage of the failures is due to trees falling over or hitting the power lines.

Table 2. Model covariates, selected for further analysis, and their possible values.

Covariate (variable)	Value
Event	1: Tor, 2: Hilde, 3: Ivar, 4: Nina
Location	1: City, 2: Urban, 3: Countryside, 4: City and urban, 5: Urban and countryside, 6: City and countryside, 7: City, countryside, urban
County	1: Finnmark, 2: Troms, 3: Nordland, 4: Nord-Trøndelag, 5: Sør-Trøndelag, 6: Møre og Romsdal, 7: Sogn og Fjordane, 8: Hordaland, 9: Rogaland, 10: Vest-Agder, 11: Øst-Agder, 12: Telemark, 13: Vestfold, 14: Buskerud, 15: Akershus, 16: Oslo, 17: Østfold, 18: Oppland, 19: Hedmark, 20: Oppland and Hedmark, 21: Hordaland and Rogaland, 22: Vest-Agder og Øst-Agder
Natural condition	1: Wind, 2: Trees/vegetation, 3: Salt, 4: Snow/ice, 5: Wet soil/ground, 6: Lightning, 7: Precipitation, 8: Avalanche, 9: Wind, trees/vegetation and lightning, 10: Wind and trees/vegetation, 11: Salt and lightning, 12: Wind and salt, 13: Wind and snow/ice, 14: Snow/ice and precipitation, 15: Wind, trees/vegetation, salt, snow/ice, lightning, 16: Wind, trees/vegetation, salt, snow/ice, 17: Wind, trees/vegetation, salt, snow/ice, lightning, avalanche, 18: Wind, trees/vegetation, lightning, 19: Wind, snow/ice, precipitation, 20: Wind, salt, avalanche, 21: Wind, trees/vegetation, salt, 22: Wind, trees/vegetation, wet soil/ground, 23: Lightning, precipitation, trees/vegetation, wind, salt, snow/ice, 24: Wind, trees/vegetation, lightning, snow/ice, 25: Wind, lightning, precipitation, salt, 26: Wind, snow/ice, trees/vegetation
FailureRegNet	0: No, 1: Yes
FailureStation	0: No, 1: Yes
CommunicationQuality	1: Poor, 2: Sufficient, 3: Good
FailureControlSystem	0: No, 1: Yes
Exercises	0: No, 1: Yes
TreeFallPercent	0% - 100%

4 RESULTS AND DISCUSSION

In order to identify the impact of different covariates on the recovery rate and recoverability of the power grid, the recoverability function was developed using AFT models, as described in the Data and Methodology section. It should be noted that the accuracy of the developed models and the range of model parameters depend, among other factors, on the number of available observations or data points and, thus, degree of freedom (Nisbet et al. 2009). According to several runs of different combinations of covariates, Table 2 presents the final model covariates that are selected for further analysis in this study.

Stata software was used to estimate the coefficients. For this purpose, the Weibull distribution was used as the underlying distribution, due to its flexibility in representing different recovery rates, including constant, increasing and decreasing. Using the list of covariates presented in Table 2, and by assuming a Weibull distribution and a Gamma-distributed shared frailty, the model was run. The results are shown in Table 3. Stata uses a maximum likelihood estimation approach to estimate the model coefficients. The statistical significance of the coefficients can be evaluated by comparing the reported p-values (see Table 3) for each coefficient against a pre-defined threshold, which is usually taken as 0.05. By considering a threshold of 0.05 for p-value, one can analyse which parameter has a significant effect on power distribution system recoverability and its recovery rate. In general, if the p-value is less than 0.05, the null hypothesis,

which says that the covariate has no significant effect, will be rejected in favour of the alternative hypothesis, which says the identified covariates have a significant effect on the recoverability. For example, as presented in Table 3, the covariate *Event* (i.e., 1: Tor, 2: Hilde, 3: Ivar, 4: Nina, with 2 being the base value) has p-values equal to 0.22, 0.7 and 0.369 for Tor, Ivar, and Nina respectively. Hence, it can be concluded that the covariate *Event* has no significant effect on the grid's recoverability. In other words, there are no significant differences between these events, and all of them have more and less the same effect on the grid's recoverability. The insignificant effect of the variable *Event* indicates that the recovery rate, recoverability and, thus, the expected recovery time are statistically independent of the type of the event, which is a valid point, as these storms took place during December and January, two months associated with very similar atmospheric and oceanographic conditions in Norway.

However, one should note that the significance level and the extent of the effects of covariates on grid recoverability, which are estimated in this study, to a great extent depend on the number of data points, which is 73. In general, the collected data should represent the real conditions. Here, according to the expert, the polar nights in northern areas could affect visibility for the recovery crew. However, there are only two incidents associated with a northern area county (Troms), one of which took place in the city area, where accessibility time could have been shorter. Hence, any interpretation of the results should be carried out with caution. To obtain more precise results, more accidents in the areas should be included in the database.

Regarding the impact of natural conditions ($NaturalCondition$)on recoverability, as presented in Table 3, only some of the conditions have a statistically significant effect, including wind and tree/vegetation, wind/snow-ice/wet-soil, lightning. However, these conditions are related to the cause of power cuts and, thus, might vary during the recovery phase. Moreover, the fact of whether the companies experienced failures in higher voltage levels and/or in the regional grid or not (i.e., $FailureRegNet$ = 0:No or 1:Yes), as well as the fact that the companies had failures in stations, which could be both transforming stations and connecting stations, independent of voltage level (i.e., $FailureStation$ = 0:No or 1:Yes) has a noticeable and significant impact on recoverability. The same argument holds for the covariate *Exercises*. However, although one expects to notice significant differences in recoverability, in terms of the quality of communication, the analysis results in this study using available data do not suggest any significant correlation. This could be due to either the lack of field data or to the recovery process in general not being very sensitive to the quality of communication among actors.

After identifying the covariates which have significate effect on the recoverability of the grids, the important question which should be answered is: how much these covariates will affect the recoverability of the grids? By having the magnitude of covariates, the future planning will be much effective. In Table 3, the column "coef." shows the regression coefficient of identified covariates. It shows the change in recovery rate due to the identified covariates. These numbers provide essential input for improving the future recovery process. For example, for location, we will find that location no. 2, which represents *urban area,* with p-value equal to 0.037, has a significant effect grid recoverability.

Regarding the shared frailty and the presence and impact of unobserved covariates, as presented in Table 3, it can be seen that the p-value for the likelihood-ratio test of the hypothesis $\theta = 0$ is 0.283, indicating that the unobserved heterogeneity is negligible. This means that the collected covariates fully reflect the real conditions under which the recovery process is taking place.

However, to illustrate the importance of always testing the impact of unobserved heterogeneity, the model was run, but this time the covariate *Exercises* was excluded from the analysis. The results are presented in Table 4. As shown, the p-value for likelihood-ratio test of the hypothesis $\theta = 0$ is 0.002, indicating the presence of unobserved heterogeneity in the model. Or it tells that there is one or more unobserved covariate (here, *Exercises*), which needs to be considered during the future planning. Moreover, a comparison between Table 3 and Table 4 shows that the regression coefficients are changed significantly, for example in no. 22 *Natural condition* (wind, trees/vegetation). The regression coefficient is changed from -2.5 to -2.7. When this situation arises, the analyst needs to review the recovery process carefully, to identify all possible missing covariates for consideration in future analysis.

The developed model has a high potential to quantify the effect of observed and unobserved covariates. However, the most available data are not collected for this type of analysis, which make its application a challenging task. For example, in this case study, the original interruption reports that the companies must complete and report to the FASIT-system contain more information than that listed in Table 2 as covariates. However, plugging all the provided information into the model, using only 73 data points, led to a high degree of freedom and, thus, to a non-converging solution. This computational issue could have been fixed by collecting a sufficiently large amount of data, which is one of the limitations in the current study. For this purpose, the model was constructed using only a number of important covariates that are expected to have significant effects on recoverability. However, given the amount of collected data and the number of model covariates, it is expected to have significant effect on any unobserved covariate. Nonetheless, the unobserved covariate effect was shown to have a significant impact on recoverability, once a covariate was deliberately removed from the list of model covariates.

Another important factor to keep in mind while analysing the results provided in Table 3 is significance level, which is indeed dependent on the number of covariates and amount of available data. In other words, the statistical interpretation of the model and identification of the range of influencing parameters, as well as the extent of their effects, depends, to a great extent, on the number of covariates used in the model and the amount of available data.

Table 3. Model coefficient with covariates listed in Table 2.

_t	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
Event						
1	1.028046	.83781	1.23	0.220	-.6140316	2.670123
3	.2861738	.7430107	0.39	0.700	-1.1701	1.742448
4	.83674	.9128939	0.92	0.359	-.9524992	2.625979
Location						
2	-1.53093	.7321808	-2.09	0.037	-2.965978	-.0958822
3	-.7558757	.6309408	-1.20	0.231	-1.992497	.4807455
5	-.8686251	.6343052	-1.37	0.171	-2.11184	.3745902
6	-1.648443	.9556707	-1.72	0.085	-3.521524	.2246366
7	-.6629752	.759607	-0.87	0.383	-2.151778	.8258271
County						
4	-2.215043	.9404198	-2.36	0.019	-4.058232	-.371854
5	-3.647929	.7092393	-5.14	0.000	-5.038013	-2.257845
6	-3.04726	.869635	-3.50	0.000	-4.751713	-1.342806
7	-3.270747	.859844	-3.80	0.000	-4.95601	-1.585484
8	-2.861533	.9030273	-3.17	0.002	-4.631434	-1.091632
9	-2.414826	.9768403	-2.47	0.013	-4.329398	-.5002547
12	-2.613753	1.013233	-2.58	0.010	-4.599653	-.6278533
14	-4.209499	.8687938	-4.85	0.000	-5.912303	-2.506694
18	-4.392309	.9380548	-4.68	0.000	-6.230862	-2.553755
20	-4.360538	.923181	-4.72	0.000	-6.16994	-2.551137
21	-2.555203	.9320204	-2.74	0.006	-4.381929	-.7284766
22	-3.281713	1.164456	-2.82	0.005	-5.564004	-.9994222
NaturalCondition						
2	-1.497308	.543355	-2.76	0.006	-2.562265	-.4323521
6	.0029784	.5076176	0.01	0.995	-.9919338	.9978907
9	-.6075864	.3337785	-1.82	0.069	-1.26178	.0466075
10	-.0465679	.2305315	-0.20	0.840	-.4984013	.4052656
11	1.77619	.5499074	3.23	0.001	.6983917	2.853989
12	-.6970775	.6481872	-1.08	0.282	-1.967501	.573346
13	-1.231593	.3807633	-3.23	0.001	-1.977875	-.4853104
14	-.0729835	.5094491	-0.14	0.886	-1.071486	.9255184
15	.245784	.5220478	0.47	0.638	-.7774109	1.268979
16	.6299441	.5508856	1.14	0.253	-.4497718	1.70966
17	.1059363	.6819122	0.16	0.877	-1.230587	1.44246
18	-.2882191	.674657	-0.43	0.669	-1.610522	1.034084
19	-1.02575	.8175962	-1.25	0.210	-2.628209	.5767095
21	.0220111	.2890767	0.08	0.939	-.5445688	.588591
22	-2.753224	.7549168	-3.65	0.000	-4.232834	-1.273614
23	0	(omitted)				
24	.6753564	.6864794	0.98	0.325	-.6701184	2.020831
25	0	(omitted)				
26	-.2486999	.5550894	-0.45	0.654	-1.336655	.8392552
1.FailureRegNet	-.5960308	.2394162	-2.49	0.013	-1.065278	-.1267836
1.FailureStation	-.4786911	.1862439	-2.57	0.010	-.8437223	-.1136598
CommunicationQuality						
2	-1.20731	1.167934	-1.03	0.301	-3.496418	1.081798
3	-1.12274	1.093496	-1.03	0.305	-3.265953	1.020474
1.FailureControlSystem	.5230183	.2092241	2.50	0.012	.1129466	.9330899
1.Exercises	.8454695	.1921927	4.40	0.000	.4687789	1.22216
TreeFallPercent	.0023817	.0030071	0.79	0.428	-.0035122	.0082755
_cons	4.675124	1.35377	3.45	0.001	2.021783	7.328465
/ln_p	1.299625	.2037711	6.38	0.000	.9002406	1.699009
/lntheta	-.2661752	.5901616	-0.45	0.652	-1.422871	.8905203
p	3.66792	.7474162			2.460195	5.468524
1/p	.2726341	.055555			.1828647	.4064718
theta	.7663048	.4522437			.2410211	2.436397

LR test of theta=0: chibar2(01) = 0.33 Prob >= chibar2 = 0.283

Table 4. Model coefficient with covariates listed in Table 2 and excluding the covariate Exercises.

_t	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
Event						
1	1.408279	.7584623	1.86	0.063	-.0782794	2.894838
3	.1467681	.7037525	0.21	0.835	-1.232561	1.526098
4	1.004677	.8484019	1.18	0.236	-.6581601	2.667514
Location						
2	-1.67496	.818511	-2.05	0.041	-3.279212	-.0707079
3	-1.083507	.7077462	-1.53	0.126	-2.470664	.3036495
5	-1.355051	.6894708	-1.97	0.049	-2.706389	-.0037134
6	-1.913905	1.021022	-1.87	0.061	-3.915072	.0872618
7	-1.067815	.7663694	-1.39	0.164	-2.569871	.4342416
County						
4	-2.456754	1.010048	-2.43	0.015	-4.436412	-.4770969
5	-3.638092	.8713631	-4.18	0.000	-5.345933	-1.930252
6	-3.771002	.9496189	-3.97	0.000	-5.632221	-1.909783
7	-3.617453	.93747	-3.86	0.000	-5.454861	-1.780046
8	-3.46762	1.004057	-3.45	0.001	-5.435537	-1.499704
9	-2.764427	1.088997	-2.54	0.011	-4.898823	-.6300315
12	-3.729887	1.184112	-3.15	0.002	-6.050703	-1.40907
14	-4.95731	.9731571	-5.09	0.000	-6.864663	-3.049957
18	-5.163519	1.057567	-4.88	0.000	-7.236312	-3.090726
20	-4.821263	1.049337	-4.59	0.000	-6.877926	-2.7646
21	-2.712613	1.051376	-2.58	0.010	-4.773272	-.6519536
22	-3.565478	1.18324	-3.01	0.003	-5.884586	-1.246371
NaturalCondition						
2	-1.360661	.6946758	-1.96	0.050	-2.7222	.0008788
6	-.5779705	.5091871	-1.14	0.256	-1.575959	.4200179
9	-.2821037	.3797377	-0.74	0.458	-1.026376	.4621685
10	-.1403828	.2715039	-0.52	0.605	-.6725207	.3917552
11	1.468806	.6152645	2.39	0.017	.2629099	2.674703
12	-.2514787	.6694731	-0.38	0.707	-1.563622	1.060664
13	-.6702752	.4281	-1.57	0.117	-1.509336	.1687853
14	-.946001	.5745301	-1.65	0.100	-2.072059	.1800572
15	.5126769	.5667224	0.90	0.366	-.5980786	1.623432
16	.4691369	.623665	0.75	0.452	-.7532241	1.691498
17	.3588291	.6742763	0.53	0.595	-.9627281	1.680386
18	-.1029516	.6797526	-0.15	0.880	-1.435242	1.229339
19	-1.585196	.8663967	-1.83	0.067	-3.283302	.1129105
21	.1677997	.3616901	0.46	0.643	-.5410998	.8766992
22	-2.53772	.7561812	-3.36	0.001	-4.019808	-1.055632
23	0	(omitted)				
24	.7953579	.7741048	1.03	0.304	-.7218596	2.312575
25	0	(omitted)				
26	.5187389	.5932845	0.87	0.382	-.6440772	1.681555
1.FailureRegNet	-.5319109	.2872808	-1.85	0.064	-1.094971	.0311492
1.FailureStation	-.3745567	.2311232	-1.62	0.105	-.8275498	.0784365
CommunicationQuality						
2	-1.536637	1.091337	-1.41	0.159	-3.675617	.6023438
3	-1.380925	.9910387	-1.39	0.163	-3.323325	.5614749
1.FailureControlSystem	.6595764	.2465005	2.68	0.007	.1764442	1.142709
TreeFallPercent	.0072869	.0035805	2.04	0.042	.0002693	.0143046
_cons	5.718609	1.508803	3.79	0.000	2.761409	8.67581
/ln_p	1.310773	.2065564	6.35	0.000	.90593	1.715616
/lntheta	.101794	.4954553	0.21	0.837	-.8692805	1.072869
p	3.70904	.7661257			2.474232	5.5601
1/p	.2696116	.05569			.1798529	.4041658
theta	1.107155	.548546			.4192531	2.923755

LR test of theta=0: chibar2(01) = 8.69 Prob >= chibar2 = 0.002

In order to analyse the type of effects that each covariate and its corresponding values have on recoverability or recovery rate, one can analyse the recovery rate model which is given by Equation (11). To this aim, a recovery time for each outage, as the dependent random variable, T_R, should be known prior to running the model and estimating the coefficients. In this study, the recovery time for each outage is a weighted averaging of the duration of outages and their corresponding number of end users, reported for each incident. In other words, Let $\boldsymbol{C} = \{C_1, C_2, \dots, C_m\}$ be the number of end users, corresponding to each incident, that experienced a power cut for a specific period of time, denoted by I_k, $k = 1,2, \dots,8$, where $\boldsymbol{I}$, a vector of time intervals in hours, is given by Equation (20):

$$\boldsymbol{I} = \{I_1, I_2, \dots, I_8\} = \{[1-6], [6-12], [12-24], [24-36], [36-48], [48-72], [72-96], [96,120]\} \text{ h} \quad (20)$$

Then, the recovery time (i.e., the duration of outage) for each reported incident can be calculated using Equation (21):

$$T_R = \frac{\sum_{k=1}^{8} C_k i_k}{\sum_{k=1}^{8} C_k} \quad (21)$$

where T_R is the recovery time of the reported incident, and i_k is the average of the outage time interval I_k.

The estimated coefficients presented in Table 3 can be used to analyse the effect of covariates on recoverability. To this aim, one can expand Equation (11), as:

$$r(t|x_k) = \beta t^{\beta-1} \exp[-\beta(\boldsymbol{AX})] \quad (22)$$

$$r(t|x_k) = \beta t^{\beta-1} \exp[-\beta(x_0 + x_1 a_1 + x_2 a_2 + \cdots)] \quad (23)$$

While parameter β in Equation (23) is the Weibull shape factor, given as $p = 3.66792$ in Table 3, the term x_0 is the constant term given in Table 3, $x_0 = 3.55204$, x_k is the covariate value, and a_k is the corresponding coefficient given in Table 3. Given the form of Equation (23), if the coefficient of a covariate is negative, it will increase the recovery rate. In other words, a covariate with a negative sign improves the recoverability of the system. This means, at a given time, the probability that the system has recovered will increase. Similarly, a positive sign for a covariate means that the system will recover with a lower probability, i.e., the system recovery rate and recoverability are reduced for those covariates with a positive sign.

For example, let us consider the covariate *Location*, which can have seven different values, as given in Table 2, i.e., *Location*: 1: City, 2: Urban, 3: Countryside, 4: City and urban, 5: Urban and countryside, 6: City and countryside, 7: City, countryside, urban. As presented in Table 3, all values of *Location* have an insignificant coefficient, except "2: Urban". Note that, in the data set, there is no incident reported relating to "4: City and urban", and the base value for *Location* is set "1: City" by default by Stata, as it is the minimum value of the covariate *Location*. According to Equation (23), the coefficient -1.53093, corresponding to *Location* 2: Urban, states that the recovery rate increases if the recovery process is taking places in urban areas compared to the base case, which is City.

As another example, as given in Table 3, the coefficient of *FailureRegNet* 1: Yes is -0.5960308, which states that the recovery rate is higher for those cases where the companies experienced failures in

higher voltage levels or in the regional grid. The negative coefficient of $FailureStation$ 1: Yes is -0.4786911, which states that the recovery rate is higher for those incidents where the failure has occurred in stations (transforming stations and/or connecting stations).

According to Equation (23), a positive coefficient will reduce the recovery rate and thus recoverability. For instance, let us consider the covariate $FailureControlSystem$ 1: Yes, which states that companies have experienced complications in their operation control system, which is an essential system used to localise failure and to reroute power supply. According to Table 3, the positive sign of the coefficient of $FailureControlSystem$ 1: Yes indicates that the recovery rate will be lower, compared to the base case where no complications in companies' operation control systems is experienced.

From a management perspective, the findings in this study can help the operator to take the necessary measures to minimize the impact of future events. For instance, trees/vegetation had a significant influence on recoverability, and thus the implementation of a better forest clearance programme could be an effective preventive measure. Where the level of accessibility is low, the most critical parts of the grid should be prioritized, in order to avoid future disturbances due to trees and vegetation hitting the power lines. Moreover, having a robust operational control system is essential in a recovery process. Many of the companies have experienced failure in those systems. Improving the reliability of such systems, for instance by adding redundant fibre lines, might increase the possibility of rerouting the power supply and, hence, increasing recoverability.

As illustrated by the above-mentioned discussion, the significance level and the estimated coefficients can be used to compare the recovery rate and, thus, recoverability for certain scenarios that involve the listed covariates. A quantitative value for the extent of the effects of the covariates on recoverability can be estimated, using Equation (7), which is beyond the scope of this study. Once such a quantitative evaluation is performed, a probabilistic risk assessment can be performed, in order to find the bottlenecks of the recovery process for budget allocations or possible improvements. Some studies (e.g., see Hasan et al. (2013)) validate the developed AFT models, by dividing the data into several groups and running the model for each group of the data. Some statistical tests are further performed to see if the estimated coefficients for each group of data are statistically equal. However, such an approach requires a huge amount of data, which was a limitation in this study. Nevertheless, the present study's probabilistic model has been developed based on principles of AFT models which are widely used and acceptable in duration analysis. In this regard, although the developed mathematical framework is acceptable, the results should be used with caution until additional data is collected in order to statistically validate the model.

5 CONCLUSION

Prediction of the recovery time of disrupted infrastructures provides us with essential inputs for developing an effective contingency plan when making important decisions in the recovery phase, in order to minimize the impact of the disruptive events. Recovery processes are complex tasks, and there are many factors that can affect such processes, including operational, environmental, organizational, as well as human, factors.

In addition to these observed risk factors, there are always other factors which the analysts may not identify or about which there might not be sufficient information at the time of the analysis. The common practice in most studies is to neglect the effects of such factors on the recovery process. Such a practice biases the analysis results and, consequently, increases the uncertainties associated with the effectiveness of any contingency plan. Here, in this paper, we extend the application of AFT models, which are used frequently in reliability engineering, in order to model the effects of observed and unobserved risk factors on the recoverability of disrupted infrastructures. The model is applied to Norwegian electric power distribution systems facing extreme weather events. In such a modelling framework, the infrastructure's recoverability is modelled as a function of time, observed and unobserved risk factors.

The developed statistical model is applied to 73 reports on power outage in the electrical power distribution grid in Norway. The model is used to model the recoverability as a function of time and some influencing parameters. The results from the case study indicate how the impact of covariates on recovery rate and recoverability can be analysed. Certain covariates increase the recovery rate and improve recoverability, or, in other words, the recovery rate is higher under certain scenarios than others. It is indicated that the recovery rate is higher if the failure has occurred in the regional grids, which is not intuitive. The reason for the increase in recovery rate is most likely due to the fact that failures in the regional grid affects more customers. Hence, if failures have occurred in the regional grid, it is likely that the repair rate will be higher, since a successful repair will have influence on a high amount of customers. As another example, the recovery rate is lower if the companies have experienced complications in their operation control system. It is crucial to have operational control system that is working when localizing failures. In addition, such systems also gives the operator the opportunity for rerouting and isolation of failures, decreasing the impact of the failure. It is also seen that the covariates $County$, $Exercises$, $FailureStation$, have a significant effect on recovery rate. The geographical areas where these four events took place have quite different characteristics, which is believed to influence the trajectory of the recovery process.

While some covariates have a significant effect on recovery rate, some other covariates, including $Event$ and $CommunicationQuality$, do not significantly influence the recovery rate. An explanation of the former could be that these four events have quite similar weather characteristics. It is a bit surprising that communication quality does influence the recovery process significantly, but it should be noted that almost all companies reported that the quality of the communication was good.

In this regard, the results of the model analysis can be used to identify the parameters affecting the recovery process of infrastructure systems, providing the operator and regulator of the infrastructure with valuable information to improve both the technical systems and the organisational aspects of the infrastructure, in order to enhance the resilience level of the sociotechnical systems as a whole. In that way, they are better prepared for future events. The studied data indicates that not all companies utilise the possibility to learn from previous disruptions. Moreover, it is clear that missing information is an ongoing challenge for the regulator and the operator of the Norwegian electric power distribution systems. Although stakeholders in Norway use the same reporting form, the level of detail provided varies. It is evident that,

in order to fully utilise the presented modelling approach and have statistically significant results, a comprehensive amount of data will be required.

6 LIMITATIONS AND FUTURE RESEARCH

The authors acknowledge that validation is a critical part of every modelling effort. The probabilistic model in this study is developed based on AFT models which are widely used approaches in duration analysis for analysing the impact of some influencing covariates on independent random variables. Validating the developed model will require many observations. One possibility could be to divide the data into two groups, and the model is then run for either of those groups, in order to estimate the model coefficients. A specification test can further be performed, to check whether or not the estimated coefficients corresponding to these two groups of data are statistically equal. However, one of the main limitations in the current study was lack of a large database. In this regard, the results of the current study should be used with caution. By using more data in the future, the model can be run again and validated. However, the findings in the study are consistent with the evaluations performed by the regulator (see Norwegian Water Resources and Energy Directorate (2013a, 2013b, 2015, 2017)).

In addition to the scarcity of data, there are also some limitations in the data collection procedure, which influence the quality of the data and the analysis results. The collected data are based on reports from the grid operators. The structure of the reports and the way the questions are formulated leave considerable room for subjective evaluations by the operator. Moreover, as some of the raw data are qualitative and descriptive, the results will, to some extent, depend on the author's interpretation in the data extraction process. The vagueness in the data will, of course, influence the reliability of the analysis.

It should be mentioned that the reports are sent from the operator to the regulating authority. Operators might try to protect their own reputation and business. Hence, there might be circumstances where the operator paints a different picture from the reality. This discussion highlights the need for a better data collection and power cut reporting procedure, which is a research gap that needs to be filled in the future. A national digital fault registration system already exists, but the data concerning influencing factors are not fully captured at the moment. In addition, to make the data more reliable, one option could be to anonymize some of the data.

ACKNOWLEDGMENTS

We wish to thank the Norwegian Water Resources and Energy Directorate (NVE) for providing us with the disruption data and for sharing valuable insight on the topic. We would also like to thank Associate Professor Yonas Z. Ayele at Østfold University College, Faculty of Engineering, for his guidance during the data collection and data extraction process.

NOTATION LIST

The following symbols are used in this paper:

AFT	Accelerated failure time
FASIT	Fault and Supply Interruption information Tool
NVE	Norwegian Water Resources and Energy Directorate
PH	Proportional hazard
TSA	Transmission System Operators
A	Coefficient vector
α_k	Covariate coefficient
$f(t)$	Probability density function
$F(t)$	Cumulative distribution function
$r(t)$	Recovery rate, which is the probability that the recovery is completed in the time interval $(t, t + \Delta t]$, when it is known that it has not been finished at time t
$R(t)$	Recoverability of a power distribution grid, described as the probability that the system can be recovered from a disruption event before time t
$S(t)$	Survival function. In the current study's scope, $S(t)$ is the probability that the recovery cannot be completed before some specified time t
x_k	Covariate
X	Covariate vector
β	Shape factor of a Weibull distribution
ε_i	The frailty of the ith group, which is a positive random number with mean equal to 1, variance θ, and the probability density function $g(\varepsilon_i)$.

DATA AVAILABILITY

Some data, models, or code generated or used during the study are available from the corresponding author by request:

- Extracted and coded data from the 73 interruptions reports
- Stata software analysis code

Some data, models, or code generated or used during the study are proprietary or confidential in nature and may only be provided with restrictions (e.g. anonymised data):

- The interruption reports completed by the distribution companies, as they include sensitive information. Data from these reports can, to a large extent, be provided in coded/anonymised form (as indicated above).

REFERENCES

Afghari, A. P., S. Washington, C. Prato, and M.M. Haque. 2019. Contrasting case-wise deletion with multiple imputation and latent variable approaches to dealing with missing observations in count regression models. Analytic Methods in Accident Research, 24, 100104.

Alvehag, K., and L. Soder. 2008. “A stochastic weather dependent reliability model for distribution systems.” In *Proc., 10th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS08), 25-29 May 2008, Rincon, Puerto Rico*. IEEE, 1-8.

Alvehag, K., and L. Soder. 2010. “A reliability model for distribution systems incorporating seasonal variations in severe weather.” *IEEE Transactions on Power Delivery*, 26, 910–919.

Ansell, J., and M. Philipps. 1997. "Practical aspects of modelling of repairable systems data using proportional hazards models." *Reliability Engineering & System Safety*, 58 (2), 165–171.

Bacon, P., and C. Hobson. 2014. *Human security and Japan’s triple disaster: Responding to the 2011 earthquake, tsunami and Fukushima nuclear crisis*. London and New York: Routledge.

Bagdonavicius, V., and M. Nikulin. 2001. *Accelerated life models: modeling and statistical analysis*. Chapman and Hall/CRC. Bakhshi, E., R.A.A. Khoei, A. Azarkeivan, M. Kooshesh, and A. Biglarian. 2017. "Survival analysis of thalassemia major patients using Cox, Gompertz proportional hazard and Weibull accelerated failure time models." *Medical journal of the Islamic Republic of Iran,* 31, 97.

Bakhshi, E., R.A.A. Khoei, A. Azarkeivan, M. Kooshesh, and A. Biglarian. 2017. "Survival analysis of thalassemia major patients using Cox, Gompertz proportional hazard and Weibull accelerated failure time models." Medical journal of the Islamic Republic of Iran, 31, 97.

Barabadi, A. 2014. "Reliability analysis of offshore production facilities under Arctic conditions using reliability data from other areas." *Journal of Offshore Mechanics and Arctic Engineering*, 136 (2), 021601.

Barabadi, A., J. Barabady, and T. Markeset. 2011. "Maintainability analysis considering time-dependent and time-independent covariates." *Reliability Engineering & System Safety*, 96 (1), 210–217.

Blanchard, B. S., D. C. Verma, and E. L. Peterson. 1995. *Maintainability: a key to effective serviceability and maintenance management*. John Wiley & Sons.

Boin, A., and A. McConnell. 2007. "Preparing for critical infrastructure breakdowns: the limits of crisis management and the need for resilience." *Journal of Contingencies and Crisis Management*, 15 (1), 50–59.

Bollinger, L. A., and G. P. Dijkema. 2016. "Evaluating infrastructure resilience to extreme weather–the case of the Dutch electricity transmission network." *European Journal of Transport and Infrastructure Research*, 16 (1).

Bradburn, M. J., T. G. Clark, S. Love, and D. Altman. 2003. "Survival analysis part II: multivariate data analysis–an introduction to concepts and methods." *British Journal of Cancer*, 89 (3), 431.

Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O’Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. Von Winterfeldt. 2003. "A framework to quantitatively assess and enhance the seismic resilience of communities." *Earthquake Spectra*, 19 (4), 733–752.

Burnard, K., and R. Bhamra. 2011. "Organisational resilience: development of a conceptual framework for organisational responses." *International Journal of Production Research*, 49 (18), 5581–5599.

Çağnan, Z., R. A. Davidson, and S. D. Guikema. 2006. "Post-earthquake restoration planning for Los Angeles electric power." *Earthquake Spectra*, 22 (3), 589–608.

Choi, J., N. Naderpajouh, D.J. Yu, and M. Hastak. 2019. "Capacity Building for an Infrastructure System in Case of Disaster Using the System's Associated Social and Technical Components." *Journal of Management in Engineering,* 35(4), 04019013.

Cimellaro, G. P., D. Solari, and M. Bruneau. 2014. "Physical infrastructure interdependency and regional resilience index after the 2011 Tohoku Earthquake in Japan." *Earthquake Engineering & Structural Dynamics*, 43 (12), 1763–1784.

Comes, T., and B. Van de Walle. 2014. "Measuring disaster resilience: The impact of hurricane Sandy on critical infrastructure systems." *ISCRAM*, 11, 195–204.

Cox, D. R. 2018. *Analysis of survival data*. Routledge.

Crowder, M. J. 2017. *Statistical analysis of reliability data*. Routledge.

Cutter, S. L., L. Barnes, M. Berry, C. Burton, E. Evans, E. Tate, and J. Webb. 2008. "A place-based model for understanding community resilience to natural disasters." *Global Environmental Change*, 18 (4), 598–606.

Dale, C. 1985. "Application of the proportional hazards model in the reliability field." *Reliability Engineering*, 10 (1), 1–14.

Dalziell, E. P., and S. T. McManus. 2004. "Resilience, vulnerability, and adaptive capacity: implications for system performance." International Forum for Engineering Decision Making (IFED), University of Canterbury, Christchurch.

Department of Defense, 1991. Military Handbook MIL-HDBK-217F - Reliability Predition of Electronic Equipment. Department of Defense, Washington D.C

Dessavre, D. G., J. E. Ramirez-Marquez, and K. Barker. 2016. "Multidimensional approach to complex system resilience analysis." *Reliability Engineering & System Safety*, 149, 34–43.

Dhillon, B. S. 1999. *Engineering maintainability: How to design for reliability and easy maintenance*. Gulf Professional Publishing.
Fagbamigbe, A. F., R. F. Afolabi, K. Y. Alade, A.S. Adebowale, and B. O. Yusuf. 2019. "Unobserved Heterogeneity in Determinants of Under-five Mortality in Nigeria: Frailty Modeling in Survival Analysis." *African Journal of Applied Statistics*, 6(1), 565-587.
Faturechi, R., and E. Miller-Hooks. 2014. "Measuring the performance of transportation infrastructure systems in disasters: A comprehensive review." *Journal of Infrastructure Systems*, 21 (1), 04014025.
Fine, J. P., and R. J. Gray. 1999. "A proportional hazards model for the subdistribution of a competing risk." *Journal of the American Statistical Association*, 94 (446), 496–509.
Francis, R., and B. Bekera. 2014. "A metric and frameworks for resilience analysis of engineered and infrastructure systems." *Reliability Engineering & System Safety*, 121, 90–103.
Ghodrati, B., and U. Kumar. 2005a. "Operating environment-based spare parts forecasting and logistics: a case study." *International Journal of Logistics: Research and Applications*, 8 (2), 95–105.
Ghodrati, B., and U. Kumar. 2005b. "Reliability and operating environment-based spare parts estimation approach: A case study in Kiruna Mine, Sweden." *Journal of Quality in Maintenance Engineering*. 11(2), 169-184.
Gutierrez, R. G. 2002. "Parametric frailty and shared frailty survival models." *The Stata Journal*, 2 (1), 22–44.
Haimes, Y. Y. 2012. "Systems-based approach to preparedness for, response to, and recovery from natural and human-made disasters." *Leadership and Management in Engineering*, 12(4), 288-298.
Hanagal, D. D. 2017. Frailty Models in Public Health. In Handbook of Statistics Vol. 37, pp. 209-247. Elsevier.
Hasan, S., R. Mesa-Arango, and S. Ukkusuri. 2013. "A random-parameter hazard-based model to understand household evacuation timing behavior." *Transportation research part C: emerging technologies*, 27, 108-116.
Hatlen, L. M., and K. Knudsen Aarrestad. 2015. "FAKTA Energi- og vannressurser i Norge 2015," Norwegian Ministry of Petroleum and Energy.
Heggset, J., G. Kjolle, and K. Sagen. 2009. "FASIT-A tool for collection, calculation and reporting of reliability data." In *Proc., CIRED 2009-20th International Conference and Exhibition on Electricity Distribution-Part 1*, IET, 1-4.
Hesam, S., M. Mahmoudi, A.R. Foroushani, M. Yaseri, and M. A. Mansournia. 2018." A cause-specific hazard spatial frailty model for competing risks data." *Spatial Statistics,* 26, 101-124.
Honfi, D., D. Lange, A. Malm, P. Mindykowski, M. Alheib, C. Bouffier, L. Cauvin, A. Willot, I. Ioannou, and B. Rød. 2017. "Technological resilience concepts applied to critical infrastructure." IMPROVER project.
Hossain, N. U. I., R. Jaradat, S. Hosseini, M. Marufuzzaman, and R. K. Buchanan. 2019. "A framework for modeling and assessing system resilience using a Bayesian network: A case study of an interdependent electrical infrastructure system." *International Journal of Critical Infrastructure Protection*, 25, 62–83.
Hosseini, S., K. Barker, and J. E. Ramirez-Marquez. 2016. "A review of definitions and measures of system resilience." *Reliability Engineering & System Safety*, 145, 47–61.
Hougaard, P. 1995. "Frailty models for survival data." *Lifetime Data Analysis*, 1 (3), 255–273.
Hougaard, P. 2016. "Modelling heterogeneity in survival data." *Journal of Applied Probability*, 28 (3), 695–701.
Ilbeigi, M. and B. Dilkina. 2017. "Statistical approach to quantifying the destructive impact of natural disasters on petroleum infrastructures." *Journal of Management in Engineering*, 34(1), 04017042.
International Electrotechnical Vocabulary (IEV) 191. 2007. "Chapter 191: dependability and quality of service." Accessed December 3, 2019. <http://std.iec.ch/iec60050 >.
Jardine, A., P. Anderson, and D. Mann. 1987. "Application of the Weibull proportional hazards model to aircraft and marine engine failure data." *Quality and Reliability Engineering International*, 3 (2), 77–82.
Kayrbekova, D., A. Barabadi, and T. Markeset. 2011. "Maintenance cost evaluation of a system to be used in Arctic conditions: a case study." *Journal of Quality in Maintenance Engineering*, 17 (4), 320–336.
Kong, J., S. P. Simonovic, and C. Zhang, C. (2019). "Sequential hazards resilience of interdependent infrastructure system: A case study of Greater Toronto Area energy infrastructure system." *Risk Analysis*, 39(5), 1141-1168.
Kumar, D., and B. Klefsjö. 1994. "Proportional hazards model: a review." *Reliability Engineering & System Safety*, 44 (2), 177–188.
Kumar, D., B. Klefsjö, and U. Kumar. 1992. "Reliability analysis of power transmission cables of electric mine loaders using the proportional hazards model." *Reliability Engineering & System Safety*, 37 (3), 217–222.
Labaka, L., J. Hernantes, and J. M. Sarriegi. 2015. "Resilience framework for critical infrastructures: An empirical study in a nuclear plant." *Reliability Engineering & System Safety*, 141, 92–105.
Lange, D., D. Honfi, J. Sjöström, M. Theocharidou, G. Giannopoulos, N. K. Reitan, K. Storesund, L. Melkunaite, H. Rosenquist, L. Peterson, R. Almeida, B. Rød, C. Bouffier, E. Serafinelli, and M. Lexin Lin. 2017a. "IMPROVER Deliverable 5.1 Framework for implementation of resilience concepts to Critical Infrastructure."
Lange, D., D. Honfi, M. Theocharidou, G. Giannopoulos, N. K. Reitan, and K. Storesund. 2017b. "Incorporation of resilience assessment in critical infrastructure risk assessment frameworks." In *Proc., 27th European Safety and Reliability Conference, ESREL 2017, 18 June 2017 through 22 June 2017*, CRC Press/Balkema, 1031-1038.
Lee, E. T., and J. W. Wang. 2003. *Statistical methods for survival data analysis*. Hoboken, NJ: John Wiley & Sons.

Liu, H., R. A. Davidson, and T. V. Apanasovich. 2007. "Statistical forecasting of electric power restoration times in hurricanes and ice storms." *IEEE Transactions on Power Systems*, 22 (4), 2270–2279.
Mannering, F. L., V. Shankar, and C.R. Bhat. 2016. "Unobserved heterogeneity and the statistical analysis of highway accident data." *Analytic methods in accident research*, 11, 1-16.
Matsuoka, T. 2015. "Unobserved heterogeneity in price-setting behavior: A duration analysis approach." *Japan and the World Economy*. 22(1), 13-20.
McEvoy, D., I. Ahmed, and J. Mullet. 2012. "The impact of the 2009 heat wave on Melbourne's critical infrastructure." *Local Environment,* 17 (8), 783–796.
Mendonça, D., and W. A. Wallace. 2006. "Impacts of the 2001 World Trade Center attack on New York City critical infrastructures." *Journal of Infrastructure Systems*, 12 (4), 260–270. https://doi.org/10.1016/j.cegh.2015.11.008
Ministry of Petroleum and Energy. n.d. "Strømnettet". Accessed September 12, 2018. <https://energifaktanorge.no/norsk-energiforsyning/kraftnett/>.
Mohammadian, A., and S. T. Doherty. 2006. "Modeling activity scheduling time horizon: Duration of time between planning and execution of pre-planned activities." *Transportation Research Part A: Policy and Practice*, 40 (6), 475–490.
Naseri, M. 2017. "On maintainability of winterised plants operating in Arctic regions." In *Proc., ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering*, American Society of Mechanical Engineers, V03BT02A018-V003BT002A018.
Naseri, M., and J. Barabady. 2016. "An expert-based approach to production performance analysis of oil and gas facilities considering time-independent Arctic operating conditions." *International Journal of System Assurance Engineering and Management*, 7 (1), 99–113.
Naseri, M., P. Baraldi, M. Compare, and E. Zio. 2016. "Availability assessment of oil and gas processing plants operating under dynamic Arctic weather conditions." *Reliability Engineering & System Safety*, 152, 66–82.
Nateghi, R., S. D. Guikema, and S. M. Quiring. 2011. "Comparison and validation of statistical methods for predicting power outage durations in the event of hurricanes." *Risk Analysis*, 31 (12), 1897–1906.
Nath, D. C., A. Bhattacharjee, and R. K. Vishwakarma. 2016. "Risk assessment in liver transplantation patients: A shared frailty parametric approach." *Clinical Epidemiology and Global Health*, 4(1), 1-15.
Neath, A. A., and J. E. Cavanaugh. 2012. "The Bayesian information criterion: background, derivation, and applications." *Wiley Interdisciplinary Reviews: Computational Statistics*, 4 (2), 199–203.
Nelson, W. B. 2009. *Accelerated testing: Statistical models, test plans, and data analysis*. John Wiley & Sons.
Nisbet, R., J. Elder, and G. Miner. 2009. *Handbook of statistical analysis and data mining applications*., Academic Press.O'Rourke, T. D. 2007. "Critical infrastructure, interdependencies, and resilience." *BRIDGE-Washington-National Academy of Engineering*, 37 (1), 22.
Orbe, J., E. Ferreira, and V. Núñez-Antón. 2002. "Comparing proportional hazards and accelerated failure time models for survival analysis." *Statistics in Medicine*, 21 (22), 3493–-3510.
Ouyang, M. 2014. "Review on modeling and simulation of interdependent critical infrastructure systems." *Reliability Engineering & System Safety*, 121, 43–60.
Ouyang, M., L. Dueñas-Osorio, and X. Min. 2012. "A three-stage resilience analysis framework for urban infrastructure systems." *Structural Safety*, 36, 23–31.
Pan, W. 2001. "Akaike's information criterion in generalized estimating equations." *Biometrics*, 57 (1), 120–125.
Peng, L., and Y. Huang. (2007). "Survival analysis with temporal covariate effects." *Biometrika*, 94 (3), 719–733.
Petersen, L., L. Fallou, P. Reilly, and E. Serafinelli. 2017. "European expectations of disaster information provided by critical infrastructure operators: Lessons from Portugal, France, Norway and Sweden." *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)*, 9 (4), 23–48.
Pursiainen, C., and P. Gattinesi. 2014. "Towards testing critical infrastructure resilience." *JRC Scientific and Policy Reports*.
Qiao, Y., S. Labi, and J. D. Fricker. 2019. "Hazard-based duration models for predicting actual duration of highway projects using nonparametric and parametric survival analysis." *Journal of Management in Engineering*, 35 (6), 04019024.
Rausand, M., and A. Høyland. 2004. *System reliability theory: Models, statistical methods, and applications*. Hoboken, NJ: John Wiley & Sons.
Rinaldi, S. M., J. P. Peerenboom, and T. K. Kelly. 2001. "Identifying, understanding, and analyzing critical infrastructure interdependencies." *IEEE Control Systems*, 21 (6), 11–25.
Rocchetta, R., Y. F. Li, and E. Zio. 2015. "Risk assessment and risk-cost optimization of distributed power generation systems considering extreme weather conditions." R*eliability Engineering & System Safety*, 136, 47–61.
Rochas, C., T. Kuzņecova, and F. Romagnoli. 2015. "The concept of the system resilience within the infrastructure dimension: application to a Latvian case." *Journal of Cleaner Production*, 88, 358–368.
Rose, A. 2004. "Defining and measuring economic resilience to disasters." *Disaster Prevention and Management: An International Journal*, 13 (4), 307–314.
Rose, A., and S. Y. Liao. 2005. "Modeling regional economic resilience to disasters: A computable general equilibrium analysis of water service disruptions." *Journal of Regional Science*, 45 (1), 75–112.

Saeed, T. U., R. Nateghi, T. Hall, and B. S. Waldorf, B. S. 2019a. "Statistical Analysis of Area-wide Alcohol-related Driving Crashes: A Spatial Econometric Approach." *Geographical Analysis*.
Saeed, T. U., T. Hall, H. Baroud, and M. J. Volovski. 2019b. "Analyzing road crash frequencies with uncorrelated and correlated random-parameters count models: An empirical assessment of multilane highways." *Analytic Methods in Accident Research*, 100101.
Seraneeprakarn, P., S. Huang, V. Shankar, F. Mannering, N. Venkataraman, and J. Milton. 2017. "Occupant injury severities in hybrid-vehicle involved crashes: A random parameters approach with heterogeneity in means and variances." *Analytic Methods in Accident Research,* 15, 41-55.
Shaon, M. R. R., X. Qin, M. Shirazi, D. Lord, and S. R. Geedipally. 2018. Developing a Random Parameters Negative Binomial-Lindley Model to analyze highly over-dispersed crash count data. Analytic methods in accident research, 18, 33-44.
The Norwegian Meteorological Institute (MET). 2015. "Ekstremverrapport ", Norwegian Meteorological Institute <https://www.met.no/publikasjoner/met-info/ekstremvaer>. Accessed 10 March 2019.
The Norwegian Water Resources and Energy Directorate (NVE). 2014a. "Erfaringer etter ekstremværet Hilde." Rapport 2014:8.
The Norwegian Water Resources and Energy Directorate (NVE). 2014b. "Erfaringar fra ekstremværet Ivar." Rapport 2014:9.
The Norwegian Water Resources and Energy Directorate (NVE). 2015. "Erfaringar frå ektremveret Nina." Rapport 2015:55.
The Norwegian Water Resources and Energy Directorate (NVE). 2017. "Erfaringer fra ekstremværet Tor. Sammenlignet med erfaringer fra Dagmar." Rapport 2017:41.
Tian, L., D. Zucker, and L.J. Wei. 2005. "On the Cox model with time-varying regression coefficients." *Journal of the American Statistical Associatio*n, 100, 172–183.
UNISDR. n.d. "Terminology on disaster risk reduction ", <https://www.unisdr.org/we/inform/terminology>. Accessed 15 September 2019.
Volinsky, C. T., and A. E. Raftery. 2000. "Bayesian information criterion for censored survival models." *Biometrics*, 56 (1), 256–262.
Wei, L.-J. 1992. "The accelerated failure time model: a useful alternative to the Cox regression model in survival analysis." *Statistics in Medicine*, 11 (14-15), 1871–1879.
Wienke, A. 2010. *Frailty models in survival analysis*. Chapman and Hall/CRC.
Yashin, A. I., J. W. Vaupel, and I. A. Iachine. 1995. "Correlated individual frailty: An advantageous approach to survival analysis of bivariate data." *Mathematical Population Studies*, 5 (2), 145–159.
Youn, B. D., C. Hu, and P. Wang. 2011. "Resilience-driven system design of complex engineered systems." *Journal of Mechanical Design*, 133 (10), 101011.
Yue, H. and K. S. Chan. "A Dynamic Frailty Model for Multivariate Survival Data". *Biometrics*. 53(3), 785 - 793.

Paper VII

Critical Infrastructures: How resilient are they?

Rød, B., and Johansson, J.

Manuscript to be submitted for possible publication in an international journal.

Revised version of the manuscript submitted to Reliability Engineering & System Safety on July 8, 2020.

Critical Infrastructures – How resilient are they?

Bjarte Rød

University of Tromsø – The Arctic University of Norway, Department of Technology and Safety, Norway. E-mail: Bjarte.rod@uit.no

Jonas Johansson

Lund University, LTH, Division of Risk Management and Societal Safety, Sweden. E-mail: jonas.johansson@risk.lth.se

Abstract: This paper reviews resilience analyses and assessments of real-life critical infrastructures (CIs) in scientific publications. Although resilience of critical infrastructures has gained considerable attention in the research literature during the last decade, the underlying thesis is that there still exist relatively few resilience studies on real-life infrastructures, varying greatly in their operationalization of the concept and with little guidance towards concluding their level of resilience. We ask the questions: how is resilience operationalized, what methods are advocated for, are CI interdependencies addressed, and is it possible to conclude towards the resilience level of different CIs? The paper hence contributes to the research field by providing an overview of critical infrastructure resilience research, introducing the essence of research in the field to new researchers and providing a summarizing account of current research for active researchers. Only a total of 50 scientific research articles were identified as relevant and subsequently reviewed, although using an open and systematic scoping approach and by utilizing the Scopus database. Only articles that explicitly stated to carry out resilience analyses of real-life infrastructures were included, although acknowledging that studies addressing for example vulnerability or recovery of infrastructures can be viewed as adding to the current state of knowledge regarding CI resilience. Associated concepts to resilience, such as robustness, reliability, survivability, rapidity, adaptation, and anticipation, is frequently used and it is explored how these are related to the concept of resilience. The approaches used for assessing CI resilience can be divided into four overarching groups: (1) empirical, (2) modelling and simulation, (3) expert, and (4) index or indicator approaches. The conceptualization of resilience varies across the articles, but where four fundamental resilience aspects can be discerned: anticipation, robustness, recovery, and adaptation. However, we conclude that most analyses tend to focus on only one or two resilience aspects simultaneously, where the clear majority focus either on robustness or recovery aspects. Only few of the reviewed articles suggests and analyse resilience enhancing measures, where most articles only conclude that the results are targeted towards such work. The overarching conclusion is that research regarding CI resilience of real-life infrastructures, and especially towards how to analyse and enhance CI resilience, is still in its infancy, where substantial efforts are needed towards being able to draw informed conclusions with respect to their level of resilience and the effect of interdependencies.

Keywords: Critical Infrastructure, Resilience, Review, Scoping Study, Applied, Real-life, Case studies.

1. Introduction

The world is becoming more complex, inducing vulnerabilities across sectors, businesses and critical infrastructures (OECD, 2019; Moteff, 2010; Rinaldi et al., 2001;). Interconnected infrastructure systems provide critical services that the society is reliant on to ensure quality of life, economic prosperity and allows for easier and faster exchange of services of various forms (OECD, 2019). Ensuring the resilience of these critical infrastructures (CIs) are hence paramount. However, infrastructure interdependencies give rise to increased complexities and the potential of cascading effects across infrastructures that could occur in the event of a disruption or a crisis (Rinaldi et al., 2001; Johansson et al., 2015). As such, addressing these interdependencies in a resilience setting is challenging, but of outmost necessity.

Past large-scale events, such as the Argentina, Paraguay and Uruguay blackout in 2019, Hurricane Sandy in 2012, the Eyjafjallajökull eruption in 2010, and the European blackout in 2006, clearly reveals both the complexities involved and the far extending impacts infrastructure disruptions have on the society they provide services to. The EU-directive from 2008, later implemented by the European Programme for CI protection (EPCIP), also highlight the cross-country scale of critical infrastructures, by stating that" there are a certain number of critical infrastructures in the community, the disruption or destruction of which would have sig-

nificant cross-border impacts. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructures". (European Council, 2008, p. 1) In 2013, after the first evaluation of EPCIP (European Commission, 2013), and also remaining in the 2019 evaluation report (European Commission, 2019), two main issues were brought up, namely: (1) how to handle CI interdependencies and (2) how to enhance CI resilience. In the last decade, there has been a clear shift, both in terms of policy and scientific interest, from the protection of critical infrastructures to the resilience of critical infrastructures. Moreover, there have been acknowledgments towards the limits of relying on sectorial approaches (silo-thinking) and moving towards more holistic cross-sector approaches (system-of-system thinking), especially when dealing with the issue of critical infrastructure interdependencies.

The definition of critical infrastructure is generally converging towards a generic joint interdisciplinary definition. The overarching theme across various definitions is that they are typically defined as structures or systems, governed and managed by a multitude of organisations at several levels, that are providing the society with essential services and where the disruption of these services leads to significant societal impacts (c.f. EU Directive, 2008; DHS, 2013, ANZCTC, 2015). On national levels, there have been several policy oriented initiatives towards the protection and resilience of infrastructures, for example: Sweden (MSB, 2013), Norway (NOU, 2016), UK (HM Government, 2015), USA (DHS, 2013), Australia and New Zealand (ANZCTC, 2015). These initiatives illustrate the wide range of different policies to enhance the protection and resilience of CIs.

Critical infrastructure resilience seems to be a more contested concept compared to critical infrastructure protection. The core of the problem might come from the vagueness of the resilience concept, where there, to this date, is no commonly agreed definition of resilience. The United Nations (UNISDR, n.d.) provide a general and broad definition of resilience, describing it as "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate, adapt to, transform and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions through risk management". The definition illustrates the temporal dimensions of resilience and that resilience can be considered as an umbrella concept embracing other used concepts.

Moreover, the definition also call attention to the fact that there could be various strategies, depending on the situation, to enhance resilience of critical infrastructures, related to the temporal dimensions of resilience – before, during and after a disruption. Typically, this includes strategies related to concepts such anticipation, robustness, response, recovery, and adaptation. Consequently, policy and regulation has started to merge and implement both protection and resilience-oriented concepts (e.g. OECD, 2019; Homeland Security, 2013). In short, the society as a whole, operators of CIs, regulators and policymakers would like services from infrastructures to be as reliable and resilient as possible, and if a disruption do occur, bounce back and recover in an efficient manner.

The increasing focus on critical infrastructure resilience has led to the development of numerous resilience analysis approaches, encompassed in resilience assessment methodologies and frameworks, across several different domains (see for instance Hosseini et al., 2016; Liu & Song, 2010). The underlying thesis of the paper is, however, that there exist relatively few scientific resilience studies with application on real-life infrastructures, varying in their operationalization of the concept and with little guidance towards how resilient CIs should or should not be.

In contrast to most previous literature, the aim here is hence to review scientific studies that are assessing the resilience of real-life critical infrastructures. To be included in the review, the articles should clearly state that they aim at analysing or assessing resilience. Broadly we aim to explore what methods are advocated for, how resilience is conceptualized, analysed, evaluated and enhanced, what conceptual overlap between resilience and related concept (such as e.g. vulnerability, reliability, risk, recovery, robustness) can be seen, and what conclusions can be drawn with respect to current state of knowledge. We also investigate to what degree interdependencies between CIs are accounted for in these studies. We further aim to draw conclusions, based on these studies, with respect to the assessed resilience level of different critical infrastructures. Finally, we also aim to contribute to the research field by providing an overview of critical infrastructure resilience research, introducing the essence of research in the field to new researches and providing a summarizing account of current research for active researchers in the field.

2. Background

2.1 Resilience and related concepts

The definition of resilience is a contested one. Fields like psychology, biology, and ecology (see e.g. Holling, 1973; Pimm, 1984; Waller, 2001) often sees resilience as a process. In contrast, resilience is in the field of engineering normally understood as system behaviour near a stable equilibrium and one often talks about how fast a system return to a steady state following a disturbance (Folke, 2016). Despite being applied in the engineering field since the early 2000s (Woods, 2015), resilience is less mature than more conventional concepts such as reliability, vulnerability and risk (Aven, 2016; Zio & Aven, 2014). As stated in the introduction, the definitions of resilience highlights that resilience has its temporal dimensions and are generally embracing already known concepts. The definition suggest that resilience and risks are concepts that enrich and support each other. While risk management has a pre-event character, resilience management more strongly emphasize on preparedness, response and the ability to recover (Rød et al., 2020), also trying to account for unwanted events and surprises (Park et al., 2013). In engineering, the classical way of describing resilience is the performance loss and recovery function introduced by Bruneau et al. (2003), depicted in Figure 1. This representation of resilience clearly reflects the temporal aspects of the concept. Figure 1 describes the performance of a system, facing a disruption or incident, over time. The performance gradually degrades over time due to normal wear and then an incident occur and the system experience a sudden drop in performance and then recovers back to normal operation, as before the incident. This representation of resilience can quite straightforwardly be applied to critical infrastructures and to illustrate the different aspects of resilience. As the review study of Hosseini (2016) reveals, there are numerous ways to separate the temporal dimensions, for instance by anticipation, absorption, robustness, response, recovery, and adaptation.

In this study, we use the following four aspects to describe resilience: anticipation, robustness, recovery, and adaptation. Anticipation refers to assessments and strategies aiming to predict future threats and hazards that could influence the system, including identifying inherent vulnerabilities (Panteli et al., 2017). Assessing the performance drop after an incident, is referred to as robustness (Bruneau, 2003), where the aim is for the system to resist and absorb impact of threats and hazards in order to minimize the disruption (Vugrin et al., 2011). Recovery are assessments or activities aimed at ensuring swifter restoration of the system during the acute phase of a disruption and the related aftermath (Youn et al., 2011). Adaptation comprise assessments and activities related to the design, redesign and implementation of measures to counteract past and future threats and hazards (Francis & Bekera, 2014). It is of course difficult to differentiate adaptation from anticipation, but here we consider adaptation to be the time directly following the ended recovery phase, when new norms and conditions are adopted to.

2.2 Operationalization and management of CI resilience

There exist numerous ways of operationalizing the concept of resilience in order to analyse and evaluate resilience of critical infrastructures. Since the time the previously mentioned performance loss function was introduced, a wide range of both methods and metrics have been proposed to assess and measure CI resilience. Yet there are no commonly accepted methods or metrics. The measurement and analysis of CI resilience, of course, depends on the methodological approach chosen, as this review will show.

In analogy with existing standards for risk management (e.g. ISO 31000:2018), a resilience assessment can be characterised by two components (Lange et al., 2017), namely resilience analysis and resilience evaluation. Resilience analysis is the process to comprehend and determine the level of resilience, while resilience evaluation is the process of comparing the results from the analysis against some predefined criteria to decide if the level of resilience is acceptable or not. Moreover, to utilize the resilience assessment results, one should propose options to enhance the resilience level, similar to risk treatment in conventional risk management.

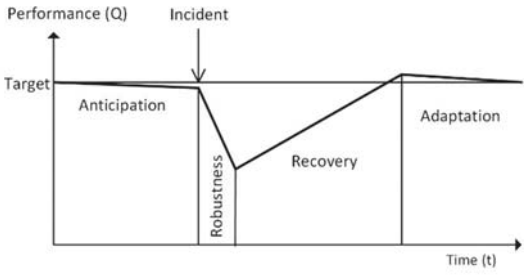

Figure 1. *Performance loss function with the four main resilience aspects.*

3. Scope of Study

There exists a relative large amount of literature related to system and engineering resilience, where the majority stems from the past decade. The scope of this study is however limited towards the scientific literature that assess resilience of real-life infrastructures, either single or independent infrastructures.

To identify and collect relevant studies, a scoping study was conducted (Arksey & O'Malley, 2005; Levac et al., 2010; Daudt et al., 2013). A systematic search using the Scopus Database was conducted in December 2019 with the search terms as given in Table 1, limiting the search to scientific journals written in English. The Scopus Database is one of the largest databases of peer-reviewed literature, with content from 24,600 active journal titles and 5,000 publishers. The search resulted in an initial list of 354 potentially relevant articles. In a second stage, the abstract and titles of the papers was subjected to a first review based on their relevance. Those papers identified as relevant for the scope of the review were in a third stage subjected to a full-text review. The fundamentals of the inclusion of articles was that they needed to express a clear connection to and use of the concept of resilience and have a clear 'real-life' critical infrastructure applied scope. The final papers for a full-review are hence in general presenting case studies of 'real-life' infrastructures by measuring, analysing or assessing resilience in some way. In the second stage 52 articles were deemed relevant. However, in the full-text review in stage three, 15 articles where deemed not to fulfil the criteria. Hence ending up with 37 included articles from the Scopus Database search. Based on references in these included articles and complementing articles of relevance known by the authors, an additional 13 articles were added. In total, 50 articles were hence included in the final review. The content of the included papers was then subjected to a structured content analysis based on a pre-defined categorization scheme of the material (see e.g. Mayring, 2004; Neuendorf, 2016).

***Table 1**. Search criteria for scoping study*

Search strings	
Query	TITLE-ABS-KEY
Concept	"Resilienc*"
Context	"Infrastruct*" w/0 "Critical" OR "Lifeline" OR "Societal" OR "Vital" OR "National" OR "Protection" OR "System"
Application	"Case stud*" OR "real-life" OR "empiric*" OR "appli*"
Constraint type of paper	
Query	DOCTYPE
Type	Journal paper (ar) OR Review (re)
Query	LIMIT-TO
Language	English (En)
Full search string	
Query	(TITLE-ABS-KEY ("Resilienc*" AND ("Infrastruct*" w/0 "Critical" OR "Lifeline" OR "Societal" OR "Vital" OR "National" OR "Protection" OR "System")) AND ("Case stud*" OR "real-life" OR "empiric*" OR "appli*")) AND (DOCTYPE (ar OR re)) AND (LIMIT-TO (LANGUAGE, "En")))

4. Results and Discussion

The papers included in this study was published between 2009 and 2020 with a distribution as seen in Figure 2. Of the total 50 included articles, only 18 addressed the issue of infrastructure interdependencies. Since critical infrastructures are highly dependent on each other, it is hence slightly surprising that the consideration of interdependencies was not addressed to a higher degree in order to achieve more comprehensive resilience assessments.

In the following sections, the findings of the review are presented and discussed in accordance to eight overarching themes, stemming from the content analysis of the articles. The reviewed literature is indexed in a separate reference list and referenced by using roman numerals within brackets. In addition, Table 10 in Appendix A provides an overview of the individual articles, with respect to the overarching themes.

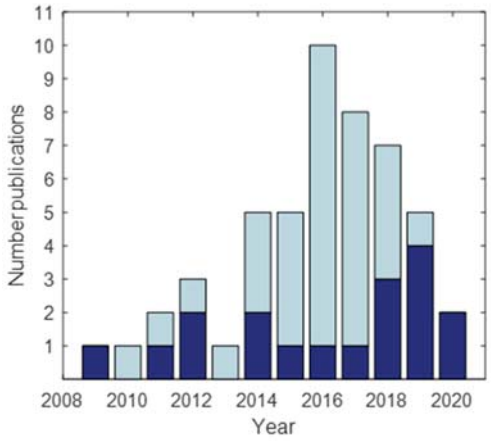

Figure 2. *No. of publications with respect to the year of publication (2008 – 2020). Consideration of interdependencies: Dark blue = yes, light blue = no.*

4.1 Addressed infrastructures

First, to give an overview of the main study areas, we classify the articles according to infrastructure sector, type, and spatial level (local, regional, national, and international). The categorization is in line with policy oriented categorization of critical infrastructures (see e.g. European Commission, 2005; DHS, 2013; Australian Government, 2010). In the categorization we distinguish between 12 infrastructure sectors, where all of these sectors, to varying degree, were covered by the included studies. The sectors were further broken down into 52 different types of infrastructures, were only 25 infrastructure types are covered in current literature. . In table 2, as a way to identify potential research gaps, we also include the sectors and infrastructure that are not addressed. It should be noted that many of the articles (n=21) covers more than one sector and several type of infrastructures, where the issue of interdependencies are also often addressed.

The results reveals that the majority of the articles investigate technical infrastructures, where the energy sector is the most dominant. Within the energy sector 28 of the articles (out of 36) addresses the electricity infrastructure. Transportation (n=31), Water & Waste (n=13), and Telecommunication and communication comes next. Surprisingly many of the articles focus at infrastructures at local levels (n=29), and less at regional level (n=10) and national level (n=10). Only one article addresses cross-national infrastructures, at this instance the global air traffic system. At the national level only Energy, Transportation and Waste & Water have been studied, while at regional level a few other sectors are covered as well.

An interesting aspect is also how many of the articles that has taken interdependency into consideration with respect to studies infrastructures, as indicated in Table 2. In total 18 of the 50 articles address interdependencies and there seems to be no clear trend of emphasis across the infrastructures sectors.

4.2 Country of application

As a continuation to the previous section, in order to provide a different perspective on the spatial level of application, the articles was also categorized with respect to country of application, depicted in Table 3.. USA is by far the country where the most studies have been carried out, close to 40% of the articles. Next comes Nepal, UK, and Sweden with respectively 9.4%, 7.5%, and 5.7%. As many as five articles are studying infrastructure resilience in Nepal, focusing on the 2011 Sikkim Earthquake and the 2015 Gorkha Earthquake that caused major damage to CIs. From an EU perspective, relatively few countries are covered (only Sweden, France, Latvia, Netherlands, Italy, Spain, and UK). This is a bit surprising considering the shift in EU policy from protection to resilience during the last years (e.g. European Commission, 2008) and the many targeted research calls on this topic. However, it could be that most of the studies at EU level are still focused towards CI vulnerability, not addressing resilience explicitly. Hence indicating a possible system lag from research calls to research output.

4.2 Hazards, threats and methodological approaches

In the research community, the common view is that resilience, as opposed to other concepts such as risk and reliability, better accounts for rare and unforeseen events, not focusing as much on specific scenarios and well-known hazards. Hence, it is interesting to see how much this is reflected in the studies, and if so, which methodological approaches capture this best. In order to this, we categorise the articles according to the hazard and threat considered and depict it against methodological approach and country of application. Four broad categories of methodological approaches could be discerned from the articles: Empirical, Modelling & Simulation, Expert, and Index. Empirical approaches typically use statistical methods to analyse historical data, e.g. constructing recovery and restoration curves.

***Table 2**. Addressed infrastructures.*

Sector	Infrastructure	Inter-national	National	Regional	Local	Sum total			
						Infrastructure		Sector	
						No. Ref	Interdep. (%)	No. Ref	Interdep. (%)
Energy	Electricity		[1],[12],[21], [30],[31],[34], [40], [42],[46*]	[8*],[10*],[11*], [16*],[33*],[49], [50*]	[6*],[9*],[14*],[15*], [17*],[19*],[22*],[23*], [26],[29*],[39],[48]	28	57,1	**33**	**48%**
	Oil & Petroleum			[16*]	[19*],[24*]	3	100		
	Gas		[21]	[8*],[50*]	[6*],[19*]	5	80		
	District heating				[7],[43]	2	0		
	Nuclear				[36]	1	0		
	Fuel supply								
Telecom & Communication	Broadband (fibre)			[16*],[50*]	[23*]	3	100	**6**	**67%**
	Mobile		[21]	[33*]	[22*]	3	66,7		
	Fixed telephony		[21]	[33*],[50*]	[22*]	4	75		
	Satellite/GNSS								
	SCADA			[10*]		1	100		
	TV								
	Radio								
	Postal								
	Newspapers								
	Social media								
	Web news								
Transportation	Road		[12]	[11*],[13],[16*], [18],[47],[50*]	[3],[15*],[20*],[22*], [24*],[25],[29*],[41]	15	53,3	**27**	**33%**
	Railway		[12],[27]	[10*],[11*]	[22*],[37]	6	50		
	Metro			[16*]	[2],[9*],[17*],[38]	5	60		
	Air	[44]			[5]	2	0		
	Maritime				[4],[35],[45]	3	0		
	Seaport								
Water & Waste	Water & Waste			[16*]		1	100	**12**	**50%**
	Water supply		[12],[21]	[8*],[50*]	[14*],[15*],[23*],[26], [28],[32],[36]	11	45,5		
	Waste water				[20*]	1	100		
	Sewage								
	Waste solid								
Food	Food supply			[16*]		1	100	**1**	**100%**
	Agriculture								
Finance	Banks			[16*]		1	100	**1**	**100%**
	Payments								
	Credit								
	Investment								
	Insurances								
Health	Hospitals			[16*]		1	100	**1**	**100%**
	Elderly care					0			
	Medicine					0			
Industry & Business	Industry			[16*]		1	100	**1**	**100%**
	Business			[16*]		1	100		
	Manufacturing					0			
	Wholesale trade					0			
	Retail trade					0			
	Warehousing					0			
Rescue	Fire & Rescue			[16*]		1	100	**1**	**100%**
	Ambulance					0			
	SOS services					0			
Public services	Governmental Services			[16*]		1	100	**2**	**100%**
	Political					0			
	Pre-schools					0			
	Schools					0			
	Universities					0			
	Shelter				[15*]	1	100		
Sum total:		**1 (2%)**	**10 (20%)**	**10 (20%)**	**29 (58%)**				

Table 3. *Country of application.*

Country	Level of application				Percent
	International	National	Regional	Local	
Global	[44]				**1.6%**
Algerie		[21]			**1.6%**
Australia			[11]		**1.6%**
Canada				[19],[22]	**3.3%**
Chile		[21]			**1.6%**
China				[20],[23],[28]	**4.9%**
Costa Rica		[21]			**1.6%**
France		[42]			**1.6%**
Iran		[21]			**1.6%**
Italy		[40]		[32]	**3.3%**
Latvia				[7],[43]	**3.3%**
Japan		[21]	[8],[50]		**4.9%**
Mexico		[21]			**1.6%**
Nepal			[13],[18]	[14],[25],[26]	**8.2%**
Netherlands		[1]			**1.6%**
New Zealand		[21]			**1.6%**
Peru		[21]			**1.6%**
Philippines		[21]			**1.6%**
South Korea		[31]			**1.6%**
Spain				[5],[36]	**3.3%**
Sweden		[12],[27]	[10]		**4.9%**
Turkey		[21]			**1.6%**
Taiwan		[21]			**1.6%**
UK		[30],[34]		[2],[17]	**6.6%**
USA		[21],[46]	[16],[33],[47], [49]	[3],[4],[6],[9],[15],[24], [29],[35],[37],[38],[39], [41],[45],[48]	**32.8%**
Percent	**1.6%**	**34.4%**	**16.4%**	**47.5%**	

Modelling & Simulation focus on system and component level analyses, i.e. by using engineering methods and network theory. Index approaches typically aggregates underlying data using indicators, often in a semi-quantitative manner. Expert approaches often gathers and analyse qualitative data using methods such surveys and interviews.

As shown in Table 4, roughly a third of the articles (n=16) takes a no hazard approach and are applied in seven countries and with one global application, where Modelling & Simulation is the dominant methodological approach. The majority of the articles (n=34), however, condition the resilience analysis on a hazard or a threat. The most prevalent hazards are earthquake (n=12), hurricane (n=9), and flooding (n=9). Not surprisingly, there is a clear connection between hazard profiles of the countries and the research application. For instance, the studies that address earthquakes are applied in the countries prone to that hazard, such as USA, Japan, Nepal, Chile, New Zealand, and Italy. In the articles with an empirical approach, the hazard focus is mainly on earthquake and hurricanes, often constructing restoration curves based on historical infrastructure failure data. Only one article address climate change and no articles were identified that covers quite common threats and hazards that historically have impacted critical infrastructures, such as fires, cyber terrorism, tornado, lightning, sabotage, and pandemic. This hence indicate a potential research gap.

4.4 Resilience: Concept, Analysis and Enhancement

To investigate if the more innovative aspects of resilience is covered, both conceptually and in the assessments, we categorize in a comparative perspective how the articles define resilience, how resilience was analysed, and what type of resilience enhancement measures were suggested. This was categorised in accordance with the four aspects of resilience as previously outlined: anticipation (An), robustness (Ro), recovery (Re), and adaptation (Ad). When describing resilience with these four aspects, it is clear that resilience closely relates to other existing concepts such as vulnerability, reliability and recoverability. Thus, we also categorise if the articles include and use related concept in addition to resilience. The use of the latter was a prerequisite for being included in the review. As the results in Table 5 reveal, a num-

Table 4. Addressed hazards and threats vs methodological approach and country of application.

Hazard	Methodological approach				%	Country
	Empirical	M&S	Index	Expert		
No hazard	[12],[46]	[2],[5],[10],[27], [29],[31],[35], [38],[40],[42], [44],[45],[47]	[36]		32%	France, Global, Italy, UK, USA, South Korea, Spain, Sweden,
Earthquake	[8],[21],[26],[39]	[4],[13],[14],[15], [18],[25],[50]		[32]	24%	Algeria, Chile, Costa Rica, Iran, Italy, Japan, Nepal, Mexico, New Zealand, USA, Peru. Philippines, Taiwan, Turkey
Hurricane	[9],[33],[37],[39],[49]	[6],[16],[19],[48]			18%	Canada, USA
Flooding		[1],[3],[17],[19], [20],[34],[43]	[22]		16%	Canada, China, Netherlands, Latvia, UK, USA
Heat wave	[11]	[1]			4%	Australia, Netherlands,
Storm		[30],[34]			4%	UK
Storm surge		[41]			2%	USA
Ice storm						
Climate change		[24]			2%	USA
Land slides		[13],[18]			4%	Nepal
Tsunami		[15]			2%	USA
Fire						
Cyber terrorism						
Physical terrorism						
Natural Hazards						
All Hazard						
Tornado						
Snow storm	[37]				2%	USA
Thunderstorm						
Lightning						
Sabotage						
Electromagnetic pulse						
Random hazard		[48]			2%	USA
Typhoon		[23]			2%	China
Intoxication		[28]			2%	China
Extreme temperatures		[7]			2%	Latvia
Sum total:	**11 (22%)**	**36 (72%)**	**2 (4%)**	**1 (2%)**		

ber of well-known concepts were used in conjunction with resilience in the articles, where recoverability (n=17), vulnerability (n=13), and robustness (n=11)constitute the majority. It is worth noting that there is only one article that directly include redundancy as a concept, which is a concept that normally is frequently mentioned in the resilience discourse.

In general, it is clear that the analysis and the proposed enhancement measures takes a narrower perspective than the definitions provided in the articles. The articles that also include either a vulnerability or reliability perspective, focus all but two only on the robustness and recovery aspects in their definition of resilience, which is then further generally consistent with how they utilize the concept for analysis and enhancement measures. The studies that include robustness and recovery, often in combination, tends to take a broader resilience perspective, both in their definition and in their analysis. Very few articles propose enhancement measures related to anticipation and adaptation. Quite many of the studies (~30%) does not provide a definition of resilience at all, which is problematic in itself. There are a few established concepts that are not used in conjunction with resilience in the articles, such risk, resourcefulness and availability.

Table 5. *Concepts vs resilience aspects in definition, analysis and enhancement.*

Concept	Reference	Sum Ref	Definition (%)				Analysis (%)				Enhancement (%)			
			An	Ro	Re	Ad	An	Ro	Re	Ad	An	Ro	Re	Ad
Resilience	**All articles**	**50**	**18**	**66**	**70**	**16**	**12**	**82**	**72**	**10**	**8**	**36**	**38**	**8**
Risk		0												
Vulnerability	[1],[2],[3],[10],[11], [24],[27],[31],[33], [41],[44],[45],[49]	13		69	54		8	100	38			38		
Reliability	[12],[20],[33],[38]	4		50	25		25	100	50	25	25	25		25
Robustness	[7],[9],[15],[17],[19], [20],[21],[22],[23], [25],[34]	11	18	64	64	27	18	100	82	18	9	36	45	9
Recoverability	[5],[6],[7],[8],[9],[13], [14],[15],[17],[18],[19], [21],[23],[34],[45], [48],[49]	17	24	71	82	24	12	65	100	12	6	24	53	6
Inoperability	[16]	1		100	100			100	100	0		100	100	
Redundancy	[22],[34]	2		100	100	50	50	100	100	50		100	100	
Flexibility	[22]	1		100	100			100	100			100	100	
Fragility	[44]	1						100						
Resourcefulness		0												
Availability		0												
Optimization		0												

4.5 Method vs Resilience aspects

To give a more nuanced picture than only the four methodological approaches, the articles were also categorised based on the method(-s) used. Similar to the previous section, these are depicted against the use of resilience in definition, analysis and enhancement, see Table 6.

The main methods utilized in the articles are network-based (n=28), either network topological (n=14) or more refined network flow methods (n=14). These articles tend to focus on the robustness and recovery aspects in their analysis, even though a few studies also consider anticipation and adaptation. The articles using engineering methods (n=3), takes a broader focus in their definition, but the analysis and enhancement measures are often mainly directed towards robustness and some towards also recovery. The articles using static or dynamic economic methods (n=4) tends to focus on robustness and recovery, and there is only one out of these articles that actually propose enhancement measures.

The articles using probabilistic methods (n=11) generally takes a broader focus, even though robustness and recovery is most dominant in the analysis and proposed enhancement measures. The articles using statistical methods (n=10) focus mostly on recovery in their analysis, which makes sense since these studies often construct restoration curves based on historical data. However, two of these articles also consider the adaptation perspective in their suggested enhancement measures. The articles using expert methods (n=6) does not consider adaptation at all for any of the three aspects (definition, analysis, and enhancement). The articles that use surveys tends to take a broader perspective, also for the enhancement measures. Only one article respectively utilizes system dynamic and discrete time models, solely focused on robustness and recovery in their definition and analysis, not at all covering any enhancement measures.

4.6 Method vs Consequences metrics of resilience

As described earlier, resilience has its temporal dimensions and associated concepts. Consequently, there are a wide range of ways to measure resilience, typically using the performance loss function. Hence, we categorize the articles in accordance with the metric used in the article to measure the drop or loss in performance, referring to the consequence of the disruption. Here we have also refined the presentation of the methods used by categorizing each article in accordance to the use of up to three main methods in the articles (i.e. single, two or three methods). The results are depicted in Table 7. Here we distinguish between five main types of metrics – functional, service, recovery, economic, and environmental – mapped against the methods used. 'Functional' means that the metrics

Table 6. Methods mapped against resilience aspects in definition, analysis and enhancement.

Method	Reference	Sum Ref	Definition (%)				Analysis (%)				Enhancement (%)			
			An	Ro	Re	Ad	An	Ro	Re	Ad	An	Ro	Re	Ad
Network topological	[2],[13],[14],[15],[18],[19],[23],[25],[29],[31],[41],[43],[44],[48]	14	21	64	71	21	7	71	71	0	7	36	57	
Network flow	[5],[6],[10],[17],[20],[23],[24],[27],[32],[34],[38],[42],[47],[50]	14	7	50	50	7	14	79	50	21	7	21	36	14
Engineering	[1],[30],[42]	3	33	67	33	33		100	33			100	33	
Static economic	[50]	1							100					
Dynamic economic	[16],[40],[46]	3		67	100			67	100			33	33	
Probabilistic	[4],[6],[7],[15],[19],[22],[28],[29],[34],[35],[48]	11	36	73	82	27	18	91	91	18	9	64	82	
Statistical	[5],[8],[9],[12],[21],[33],[37],[39],[46],[49]	10	20	70	80	20		70	100	10		20	20	20
Expert elicitation	[11],[13],[18],[22],[35],[36]	6	17	50	83		33	67	67		17	33	50	
Optimization	[24],[27],[42],[43]	4		50	50			75	25			25	25	
Monte-Carlo	[13],[30]	2	50	50	100	50		50	100			50	100	
Surveys	[11],[22],[26],[37],[50]	5	20	60	60	20	40	80	80	20	20	80	60	40
System Dynamics	[3]	1		100	100			100	100					
Discrete time model	[45]	1		100	100			100	100					

tries to capture the functionality of the infrastructure in terms of for example network oriented metrics such as largest connected subgraph or more engineering metrics such as loss of load. 'Service' is here used for metrics trying to capture the drop of service by the system such as customers or vital societal functions impacted. 'Recovery' is used for metrics trying to capture for example the time perspective of the interruption or demand on resources for recovery operation. 'Economic' are used when the metric described monetary consequence, and finally 'Environmental' is used when the metric tries to capture the impact on the environment such as for example increased CO2-emissions.

As seen 'functional' (n=27) and 'service' (n=29) are the most dominant consequence metric, followed by 'recovery' (n=10). Most articles use several methods and consequence metrics in combination. Notably, quite many of the network-based studies use both 'service' and 'recovery' metrics.

4.7 What is the level of resilience?

As a the second to last analysis of the reviewed articles, we here aim to give an account if the articles in the end gives any statements of the assessed resilience level of the infrastructure(s) under study. These accounts can be both in terms of a quantitative or qualitative form. Moreover, it is interesting to investigate if the articles provide any conclusion on the analysed resilience, e.g. if the level of resilience of the analysed infrastructure(s) is deemed as acceptable or tolerable. Here we distinguish between resilience indication, resilience assessment, and resilience comparison. Indication means that there are some, often vague, accounts of the level of resilience and why the given resilience level is achieved (e.g. through protection, responsiveness or recovery actions in place). Assessment means that clear evaluations are performed where the results are typically compared against some target value. Comparison means that the level of resilience of the analysed infrastructure(s) are contrasted against similar or other type of infrastructures.. Similar to Section 4.1, the results are depicted against sector and infrastructure. Moreover, taking into account the hazard and threat aspects brought up in Section 4.2, it is indicated (with superscripts) whether the assessed level of resilience are conditioned on the hazard or threat under study (H) or the vulnerability or no hazard analysis carried out (V).

The results, as shown in Table 8, surprisingly, reveal that the majority of the articles (n=31) do not provide any conclusion at all from their resilience analysis of the real-life infrastructure(-s) under study. Six articles

give indications, five articles provide full assessment, and eight articles provide a comparison. Some conclusions with respect to the level of resilience can only be drawn for electricity infrastructures (i.e. having more than one reference that makes statement about the resilience level). Based on the articles where a full assessment is done, the electricity infrastructure is in most cases considered to be highly resilient. Most resilience level conditions are conditioned on a hazard (n=16). In the eight articles that makes a comparison of different type of infrastructures, electricity is often the infrastructure that score best. This infrastructure is typically followed by water and telecommunication. However, as some studies indicate, these are typically highly dependent on electricity, hence causing potential delays in the recovery processes. Gas infrastructures is generally regarded at having a lower level of resilience, at least in comparison to electricity, telecommunication, and waste & water. Some studies point out that the main reason is due to the extensive repair actions that is required for such systems when disrupted.

Table 7. *Consequence metric used in methods (single, two or three methods).*

	Methods(s)	Consequence metrics				
		Functional	Service	Recovery	Economic	Environmental
One	Network topological	[25],[31],[41],[44]	[2]	[14*]		
	Network flow	[20*],[32],[38]	[10*],[17*],[20*],[32],[47]		[47]	[47]
	Engineering		[1]			
	Dynamic economic	[16*]			[40]	
	Probabilistic	[4],[7]	[4],[28]	[7]	[7]	
	Statistical	[33*],[49]	[8*],[9*],[12],[21],[39]	[33*],[39],[49]		
	Expert elicitation					
	Surveys	[26]	[26]	[26]		
	System Dynamics	[3]			[3]	
	Discrete time model		[45]	[45]		
Two	Network topological & Network flow	[23*]	[23*]			
	Network topological & Probabilistic	[15*],[19*],[48]	[15*],[19*],[29*]		[15*]	
	Network topological & Expert elicitation			[18]		
	Network topological & Optimization	[43]	[43]			
	Network flow & Probabilistic	[6*],[34]	[34]			
	Network flow & Statistical		[5]			
	Network flow & Optimization	[24*]	[24*],[27]			
	Engineering & Monte-Carlo	[30]		[30]		
	Dynamic economic & Statistical	[46*]				
	Probabilistic & Expert elicitation	[35]				
	Statistical & Surveys		[37]			
	Expert elicitation & Surveys	[11*]	[11*]			
Three	Network topological, Expert elicitation & Monte-Carlo			[13]		
	Network flow, Engineering & Optimization	[42]				
	Network flow, Static economic & Surveys		[50*]			
	Probabilistic, Expert elicitation & Surveys		[22*]			

Table 8. *Level of resilience.*

Sector	Infrastructure	No Conclusion	Indications	Assessment	Comparison
Energy	Electricity	[10],[11],[17],[19],[22], [23],[26],[30],[31],[33],[40],[42],[46],[50]	[8H],[34H],[39H]	[1H],[6H],[48H], [49H]	[9H],[12H],[14H], [15H],[16H],[21H], [29V]
	Oil & Petroleum	[19],[24]			[16H]
	Gas	[19],[50]	[8H]	[6H]	[21H]
	District heating	[7],[43]			
	Nuclear				[36V]
Telecom	Broadband (fibre)	[23],[50]			[16H]
	Mobile	[22],[33]			[21H]
	Fixed telephony	[22],[33],[50]			[21H]
	SCADA	[10]			
Transportation	Road	[3],[11],[13],[18],[20], [22],[24],[41],[47], [50]	[25H]		[12H],[15H],[16H], [29V]
	Railway	[10],[11],[22],[37]	[27V]		[12H]
	Metro	[17],[38]	[2V]		[9H],[16H]
	Air	[5]		[44V]	
	Maritime	[4],[35],[45]			
Water & Waste	Water & Waste				[16H]
	Water supply	[23],[26],[28],[32], [50]	[8H]		[12H],[14H],[15H], [21H],[36V]
	Waste water	[20]			
Food	Food supply				[16H]
Finance	Banks				[16H]
Health	Hospitals				[16H]
Industry & Business	Industry				[16H]
	Business				[16H]
Rescue	Fire & Rescue				[16H]
Public services	Governmental Services				[16H]
	Shelter				[15H]
Sum articles:		**31**	**6**	**5**	**8**

4.8 How is resilience suggested to be enhanced?

Based on the results of a resilience analysis/assessment, similar to risk treatment in risk management, the next logical step is to propose resilience enhancement and improvement options. Hence, we categorize the articles with respect to if measures were merely suggested or if the effect of the suggested measures also were analysed, as depicted in Table 9. Only about half of the articles either suggest or analyse enhancement measures (n=26). Of the studies that propose measures, even fewer actually analyse their effects (n=12). Measures targeted towards increasing structural or functional capacity to enhance resilience are most frequently proposed. Structural capacity typically includes changing network configuration, for instance by adding redundancy in terms of adding system components, while functional capacity is measures for example directed towards increase in component capacity or demand side management. Relatively few studies (n=5), uses protection as a measure to increase resilience. Given the inherent notion of the concept of resilience, it is however surprising that even this many articles suggest protection measures as means to enhance critical

infrastructure resilience. Organisational measures of different types, and buffers towards dependencies or in terms of resources, are proposed in a quarter of the articles (n=15). These types of measures relate for example to increase in human resources, optimization of organisational procedures, increased access to and warehousing of equipment and spare parts.

Table 9. *Resilience enhancement measures*

Proposed measures	Suggested	Analysed
Protection	[2],[16],[37]	[1],[22],[34]
Retrofitting		[15],[48]
Structural Capacity	[2],[4],[11],[20],[28],[31],[37],[49]	[5],[22],[30],[34],[42],[48]
Functional Capacity	[2],[4],[11],[16],[20],[28]	[1],[5],[32]
Organizational increase	[36]	[15],[19],[30],[34]
Organizational processes	[13],[18],[29],[43]	[5],[32]
Buffers - Dependencies	[11],[16]	
Buffers - Resources	[28],[29]	[19],[22],[23]
Monitoring		[48]
Demand management	[20]	
Policy		
Alternative supply		[15]
Recovery timing	[31]	
Smart strategies		[30]
Articles where measures were not addressed		
[3],[7],[8],[9],[10],[12],[14],[17],[21],[24],[25],[26],[27],[33],[35],[38],[39],[40],[41],[44],[45],[46],[47],[50]		

5. Concluding discussion

5.1 How is resilience conceptualized, analysed, and enhanced?

The results from the review indicate that there are numerous ways to conceptualize resilience. Most of the articles provide a resilience definition in their introductory parts, including the most common aspects of such a definition. Many also acknowledge more process-oriented aspects, such as anticipation and adaptation. However, this is, a bit surprisingly, seldom reflected in the analysis part of the articles. The analysis normally takes a narrower perspective, often only focusing on robustness and recovery. For instance, Whitman et al. [27] defines resilience as "[...] the ability of a system to withstand, adapt to, and recover in a timely manner from the effects of a disruptive event", while the analysis only focus on robustness. Ouyang & Wang [6] focus only on the recovery part of CIs in their resilience analysis, but define resilience as "the joint ability of infrastructure systems to resists (prevent and withstand) any possible hazard, absorb initial damage, and recover to normal operations". However, there are articles that manage to capture the broader aspects, both in their definition and in their analysis. For instance, Zhu et al. [26] define resilience as "[...] the ability of communities to prepare and plan for, absorb, recover from, and more successfully adapt to disasters", and analyse eight so-called success factors for achieving resilience: vulnerability, anticipation, redundancy, adaptive capacity, rapidity, resourcefulness, cross-scale interactions, and learning culture. These examples illustrate the multi-conceptual landscape of resilience.

The results further revealed that many concepts are used in conjunction with resilience and that many studies aim for resilience analyses, but then fall back to more conventional concepts such as vulnerability, reliability and robustness. This is connected to the fact that many of the studies take a narrower focus in their resilience analysis, compared to their conceptual definition. For instance, Kim et al. [38], apply a classical reliability method, although referring to it as a resilience analysis. Similar, Testa et al. [41] identifies critical links and nodes in a transportation network to measure resilience, hence addressing vulnerabilities rather than actually providing a resilience analysis.

In general, with respect to approaches and methods used, we find the same trend. There seems to no single analysis method that manage to capture all the four resilience aspects (anticipation, robustness, recovery, and adaptation). For instance, Espinoza et al. [34] covers all four aspects in their analysis, but in order do so probabilistic and network flow

methods are used separately, rather than in an integrated manner, also by including several resilience metrics. The qualitative methods (expert and index), tends to cover, to larger extent, adaptation and anticipation in a single method analysis. The results further reveal that the aspects of robustness and recovery is dominating the Modelling & Simulation and Empirical approaches, and thus some central aspect of resilience might be missing and not well captured with these approaches. This leads to the notion that, in spite of the growth in the demand of and research on critical infrastructure resilience analysis methodologies, the innovative potential of resilience as a concept is not fully utilised in current literature.

Three quarters of the analyses in the articles are conditioned on some hazard or threat, while the remaining one fourth are conditioned on a vulnerability or no hazard perspective. This finding add an interesting perspective to the debate whether resilience is dependent on detailed hazard scenarios or not (see e.g. Cutter et al. 2016; Aven, 2016; Aven, 2019). The results further revealed that only a relatively few quite common hazards were considered. Most of the articles base their analyses on some hazard that historically has caused major damage to CIs, such as flooding, hurricane, and earthquake. The articles rarely address emerging threats and rare events. For instance, there are no articles that analyse the effect of cyber-attacks, although a growing concern around the world, and pandemics, of great relevance given the Covid19-pandemic. The rather narrow scope of hazards and threats addressed hence constitute a clear research gap in the literature. The reason for this narrow focus could be associated with the conceptual approaches being used. It seems like conventional 'risk-thinking' is still prevalent in the studies, with the tendency of excluding surprising and rare events. To that end, the articles that focus on vulnerability tends to better capture the central aspects of resilience.

There are also surprisingly few articles that suggest any resilience enhancement measures and even fewer that analyse the effect of these measures. Many articles indicate in their discussion or concluding remarks some possible measures that could enhance the resilience level, without drawing any conclusion towards their possible effects. Current state in the literature seems to be a focus on proposing analysis (or assessment) methods and declaring their usefulness, with occasional brief highlights that the results can be useful for decision-making. A conclusion of the review of greater concern is therefore the fact that very few articles provide any conclusion on outcome of their analysis of real-life infrastructures. The implication of this finding, connecting back to the title of the paper, is further discussed the following section.

5.2 What is the level of resilience?

In the initial search, 354 articles were identified as potentially relevant. However, there were only very few articles out of these that actually made an assessment of real-life CIs. Most of the articles that were not included only provided a simplified demonstration of their assessment methodology for illustrative purposes. Of the 50 articles included in the full review, only five of them made a full resilience assessment and provided an evaluation of the analysis results. Hence, it is very hard to draw any clear-cut conclusion with respect to the level of resilience of CIs. However, quite many articles made some comparison against other infrastructures or at least presented some indications.

The results revealed that electricity infrastructures, in general, are assessed to have a rather high level of resilience and belong to the most resilient type of infrastructure. However, the results are often dependent on hazard scenarios, and some exceptions are found. For instance, Nazarnia et al. [14] state in their final remarks that "water infrastructure is more resilient than electric power infrastructure" conditioned on the Bhaktapur earthquake. Similar, Kameshwar et al. [15] comes to the conclusion that "comparison between different infrastructures systems show that transportation system is one of the more resilient systems [...], while electric power networks (EPN) and water systems are least resilient and, therefore, govern the resilience of the combined infrastructure system". The latter example is quite illustrative for many of the reviewed articles. The infrastructures are compared against each other and even sometimes analysed as system-of-system by including interdependencies, but it is hard to tell if the analysed resilience level is regarded as satisfactory or not. Moreover, it is interesting to note that most articles present no conclusion or only provides vague statements. For instance, Zhao et al. [28] states "with the proposed assessment method decision makers can evaluate the resilience of a system under specific disruption scenarios, which can provide guidance on how to schedule during the disruption event", without proposing any specific enhancement measures or stating anything about the assessed level of resilience. However, a few articles provide specific

recommendations, such Fotouhi et al. [29] who states that "the results show that for the given scenarios, investment in the transportation network is most critical, and using some budget for the power network is most important at lower budget levels".

As the study reveals, relatively few hazards are addressed in the identified literature. Moreover, most articles focus on hazards and threats that CIs are frequently exposed to. Hence, it is difficult to tell to what level CIs are also resilient towards more low probability events and against new and emerging hazards and threats. For instance, we found only one article addressing climate change and no article that consider cyber terrorism, tornado, lightning, sabotage, and pandemic – which potentially could cause significant losses in CI performance and entail great societal consequences.

The list of CIs is long and many are not addressed in the identified literature, such as fuel supply, seaports, satellite systems, and agriculture. Food supply is only considered in one of the articles. The majority of the articles considers electricity, transportation and waste & water infrastructures. The reason for this could be that operators of these CIs have better procedures for collecting and recording data as indicated in [12] and hence more easily lends themselves for analyses. Moreover, quite surprisingly given the often national and cross-national perspectives in CI policies, most of the articles considers CIs on local and regional spatial levels, and very few at a national and cross-national spatial levels. At an international level, the only infrastructure studied is the air traffic infrastructure. This could also be linked to data collection barriers and the sensitive nature of the data, especially at cross-national spatial levels.

To summarize, above leads to two major concerns. First, if there is no clear assessment on whether the resilience is acceptable or not, it is difficult to provide any guidance towards the need of resilience enhancement measures. Secondly, given these results, current state of scientific resilience analyses of real life infrastructures provides very little guidance towards forming policy actions. It is hence clear that the scientific resilience research on real-life infrastructures is still in its infancy.

5.3 Limitation of Study

There are two main aspects that could potentially influence the quality of this scoping study and the validity of the conclusions drawn.

First, with respect to completeness of the study, it is to some degree uncertain if all relevant studies have been identified. We tried to minimize this uncertainty by using a broad search string in one of the largest available databases for scientific publications to capture as many articles as possible. This lead to the initial identification of 354 potentially relevant articles, where only 37 of these were deemed relevant for a full-text review given the aim of the study. Additional 13 articles were identified based on references in the articles or through prior knowledge by the authors. Hence, it is our belief that the scoping has a high degree of completeness and the conclusions drawn with respect to this have a high degree of validity.

Second, utilizing a categorization scheme for the content analysis means that other potentially relevant aspects of the articles were not assessed. We tried to address this by letting the content of the articles iteratively influence the categorization scheme as to include as many and as correct categorizations as possible. However, fitting the content of an article into specific categories comes occasionally with a degree of subjective judgement calls. Hence, resulting in the possibility of misinterpretation of the aim or content of the articles. We tried to minimize this uncertainty by iteratively refining the categorization scheme and by also allowing for multiple instances for a specific categorization, for example allowing for categorization of multiple methods and not only the main method used. Hence, we argue, with the aim of the article in mind, that the content is well accounted for and that the conclusions drawn holds validity.

5.4 Research opportunities

This study has identified several research gaps in the field, which opens up for future research opportunities. The main research gaps identified are related to the sparse completeness of the type of infrastructures addressed, the hazard and threats included, and the spatial level of the analyses. Moreover, methodologically we see that hardly any single method manages to capture all the four outlined aspects of resilience, instead there seems to be a need for combining several methods. How to do so for comprehensive real-life infrastructure assessments needs further attention. Finally, the study reveals that the latter part of an infrastructure resilience assessment, namely resilience evaluation, seems to be largely underresearched. Finally, it is also clear that the resilience con-

cept is still a contested one, and more research towards stronger conceptualization and operationalization are also deemed necessary. Hence, we suggest that future research should focus on closing these identified main gaps, where indications of further research opportunities have also been highlighted throughout the article.

6. Conclusions

This study has put forward evidence that it is very hard, based on current academic literature, to come to any clear-cut conclusion with respect to the current level of resilience of real-life critical infrastructures, and even harder on adequate ways on how to enhance their resilience. Hence, the question set out in the title of the paper hence largely remains unanswered – presenting challenges for scientific guidance of policy actions and decision-making.

We also conclude that there exist several other clear research gaps, the main ones being the scarce completeness of studies when it comes to type of infrastructures, hazards and spatial levels addressed together with a need of further work toward conceptualization and operationalization of resilience.

The overarching conclusions is that much research is needed towards analysing, evaluating and enhancing real-life critical infrastructure resilience, especially when it comes to the interdependent nature of critical infrastructures.

Acknowledgement

This work was part of the Centre for Critical Infrastructure Protection Research (CenCIP) in Sweden, funded by the Swedish Civil Contingencies Agency (MSB), and the IMPROVER project, funded from the European Union Horizon 2020 research and innovation program under grant agreement no. 653390. This support is gratefully acknowledged.

References

ANZCTC. (2015). National Guidelines for Protecting Critical Infrastructure from Terrorism, Australia-New Zealand Counter-Terrorism Committee, ISBN: 978-1-925290-43-1.

Arksey, H., & O'Malley, L. (2005). Scoping studies: towards a methodological framework. International journal of social research methodology, 8(1), 19-32.

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

Aven, T. (2019). The call for a shift from risk to resilience: What does it mean?. Risk Analysis, 39(6), 1196-1203.

Aven, T., & Zio, E. (2014). Foundational issues in risk assessment and risk management. Risk Analysis, 34(7), 1164-1172.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., ... & Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. Earthquake spectra, 19(4), 733-752.

Cutter, S. L. (2016). Resilience to what? Resilience for whom?. The Geographical Journal, 182(2), 110-113.

Daudt, H. M., van Mossel, C., & Scott, S. J. (2013). Enhancing the scoping study methodology: a large, inter-professional team's experience with Arksey and O'Malley's framework. BMC medical research methodology, 13(1), 48.

DHS. (2013). NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience, Department of Homeland Security, USA

European Commission. (2005). *Green paper on a european programme for critical infrastructure protection* (COM(2005) 576 final). Brussels, Belgium. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN

European Commission. (2013). Commission staff working document on a new approach to the European programme for critical infrastructure protection making European infrastructures more secure. (SWD(2013) 318 final). Brussels, Belgium. Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

European Commission. (2019). Commission staff working document. Evaluation of council directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (SWD(2019) 308 final). Brussel, Belgium. Retrieved from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190723_swd-2019-308-commission-staff-working-document_en.pdf

European Council. (2008). On the identification and designation of european critical infrastructures and the assessment of the need to improve their protection (Council Directive 2008/114/EC of 8 December 2008).

Folke, C. (2006). Resilience: The emergence of a perspective for social–ecological systems analyses. Global environmental change, 16(3), 253-267.

Francis, R., & Bekera, B. (2014). A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering & System Safety, 121, 90-103.

HM Government. (2015). National Security Strategy and Strategic Defence and Security Review 2015

- A Secure and Prosperous United Kingdom, HM Government, ISBN: 9781474125963.
Holling, C. S. (1973). Resilience and stability of ecological systems. Annual review of ecology and systematics, 4(1), 1-23.
Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47-61.
ISO (International Organization for Standardization). (2018). Risk management – Guidelines. ISO 31000:2018. Geneva, Switzerland.
Johansson, J., Hassel, H., Cedergren, A., Svegrup, L., Arvidsson, B., (2015). Method for describing and analysing cascading effects in past events: Initial conclusions and findings, ESREL 2015, Zürich, Switzerland, September 7-10.
Lange, D., Honfi, D., Theoharidou, M., Giannopoulos, G., Kristina, N., & Storesund, K. (2017). Incorporation of resilience assessment in critical infrastructure risk assessment frameworks. Paper presented at the 27th European Safety and Reliability Conference.
Levac, D., Colquhoun, H., & O'Brien, K. K. (2010). Scoping studies: advancing the methodology. Implementation science, 5(1), 69.
Mayring, P. (2004). Qualitative content analysis. A companion to qualitative research, 1, 159-176.
Moteff, J. (2010). Critical Infrastructures: Background, Policy, and Implementation (RL30153). Congressional Research Service: Report, 1-38.
MSB. (2013). Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, Swedish Civil Contingencies Agency, ISBN: 978-91-7383-447-6.
Neuendorf, K. A. (2016). The content analysis guidebook. Sage. California, USA.
Norges offetnlige utredninger (NOU). (2016). Samhandling for sikkerhet. Beskuttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid. NOU 2016:19. Oslo, Norway. ISBN 978-82-583-1295-3.
OECD (The Organisation for Economic Co-operation and Development). (2019). Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies, OECD Publishing, Paris. https://doi.org/10.1787/02f0e5a0-en
Pant, R., Barker, K., & Zobel, C. W. (2014). Static and dynamic metrics of economic resilience for interdependent infrastructure and industry sectors. Reliability Engineering & System Safety, 125, 92-102.
Panteli, M., Trakas, D. N., Mancarella, P., & Hatziargyriou, N. D. (2017). Power systems resilience assessment: Hardening and smart operational enhancement strategies. Proceedings of the IEEE, 105(7), 1202-1213.
Pimm, S. L. (1984). The complexity and stability of ecosystems. Nature, 307(5949), 321.
Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE control systems magazine, 21(6), 11-25.
Rød, B., Lange, D., Theocharidou, M., & Pursiainen, C. (Forthcoming 2020). From Risk Management to Resilience Management in Critical Infrastructure. Journal of Management in Engineering. DOI: 10.1061/(ASCE)ME.1943-5479.0000795
UNISDR. (n.d.). Terminology on disaster risk reduction Retrieved from https://www.unisdr.org/we/inform/ terminology. Accessed 25 October 2019.
U.S Department of Homeland Security. (2013). National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience. Accessed 29 April 2020. Available at https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
Vugrin, E. D., Warren, D. E., & Ehlen, M. A. (2011). A resilience assessment framework for infrastructure and economic systems: Quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. Process Safety Progress, 30(3), 280-290.
Waller, M. A. (2001). Resilience in ecosystemic context: Evolution of the concept. American journal of orthopsychiatry, 71(3), 290-297.
Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering & System Safety, 141, 5-9.
Youn, B. D., Hu, C., & Wang, P. (2011). Resilience-driven system design of complex engineered systems. Journal of Mechanical Design, 133(10).

Reviewed literature

[1] Bollinger, L. A., & Dijkema, G. P. (2016). Evaluating infrastructure resilience to extreme weather–the case of the Dutch electricity transmission network. European Journal of Transport and Infrastructure Research, 16(1).
[2] Chopra, S. S., Dillon, T., Bilec, M. M., & Khanna, V. (2016). A network-based framework for assessing infrastructure resilience: a case study of the London metro system. Journal of The Royal Society Interface, 13(118), 1-11.
[3] Croope, S. V., & McNeil, S. (2011). Improving resilience of critical infrastructure systems postdisaster: recovery and mitigation. Transportation research record, 2234(1), 3-13.
[4] Shafieezadeh, A., & Burden, L. I. (2014). Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports. Reliability Engineering & System Safety, 132, 207-219.
[5] Voltes-Dorta, A., Rodríguez-Déniz, H., & Suau-Sanchez, P. (2017). Passenger recovery after an airport closure at tourist destinations: A case study of Palma de Mallorca airport. Tourism Management, 59, 449-466.

[6] Ouyang, M., & Wang, Z. (2015). Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. Reliability Engineering & System Safety, 141, 74-82.

[7] Feofilovs, M., & Romagnoli, F. (2017). Resilience of critical infrastructures: probabilistic case study of a district heating pipeline network in municipality of Latvia. Energy Procedia, 128, 17-23.

[8] Cimellaro, G. P., Solari, D., & Bruneau, M. (2014). Physical infrastructure interdependency and regional resilience index after the 2011 Tohoku Earthquake in Japan. Earthquake Engineering & Structural Dynamics, 43(12), 1763-1784.

[9] Comes, T., & Van de Walle, B. (2014). Measuring disaster resilience: The impact of hurricane sandy on critical infrastructure systems. ISCRAM, 11, 195-204.

[10] Johansson, J., Hassel, H., & Cedergren, A. (2011). Vulnerability analysis of interdependent critical infrastructures: case study of the Swedish railway system. International journal of critical infrastructures, 7(4), 289-316.

[11] McEvoy, D., Ahmed, I., & Mullett, J. (2012). The impact of the 2009 heat wave on Melbourne's critical infrastructure. Local Environment, 17(8), 783-796.

[12] Johansson, J., Bjärenstam, R. J., & Axelsdóttir, E. (2018). Contrasting critical infrastructure resilience from Swedish infrastructure failure data. In Safety and Reliability–Safe Societies in a Changing World (pp. 1287-1295). CRC Press.

[13] Aydin, N. Y., Duzgun, H. S., Heinimann, H. R., Wenzel, F., & Gnyawali, K. R. (2018). Framework for improving the resilience and recovery of transportation networks under geohazard risks. International journal of disaster risk reduction, 31, 832-843.

[14] Nazarnia, H., Sarmasti, H., & Wills, W. O. (2020). Application of household disruption data to delineate critical infrastructure resilience characteristics in the aftermath of disaster: A case study of Bhaktapur, Nepal. Safety science, 121, 573-579.

[15] Kameshwar, S., Cox, D. T., Barbosa, A. R., Farokhnia, K., Park, H., Alam, M. S., & van de Lindt, J. W. (2019). Probabilistic decision-support framework for community resilience: Incorporating multi-hazards, infrastructure interdependencies, and resilience goals in a Bayesian network. Reliability Engineering & System Safety, 191, 106568.

[16] Cimellaro, G. P., Crupi, P., Kim, H. U., & Agrawal, A. (2019). Modeling interdependencies of critical infrastructures after hurricane Sandy. International Journal of Disaster Risk Reduction, 38, 101191.

[17] Goldbeck, N., Angeloudis, P., & Ochieng, W. Y. (2019). Resilience assessment for interdependent urban infrastructure systems using dynamic network flow models. Reliability Engineering & System Safety, 188, 62-79.

[18] Hossain, N. U. I., Jaradat, R., Hosseini, S., Marufuzzaman, M., & Buchanan, R. K. (2019). A framework for modeling and assessing system resilience using a Bayesian network: A case study of an interdependent electrical infrastructure system. International Journal of Critical Infrastructure Protection, 25, 62-83.

[19] Kong, J., Simonovic, S. P., & Zhang, C. (2019). Sequential hazards resilience of interdependent infrastructure system: A case study of Greater Toronto Area energy infrastructure system. Risk Analysis, 39(5), 1141-1168.

[20] Yang, Y., Ng, S. T., Zhou, S., Xu, F. J., & Li, H. (2019). Physics-based resilience assessment of interdependent civil infrastructure systems with condition-varying components: A case with stormwater drainage system and road transport system. Sustainable Cities and Society, 101886.

[21] Kammouh, O., Cimellaro, G. P., & Mahin, S. A. (2018). Downtime estimation and analysis of lifelines after an earthquake. Engineering Structures, 173, 393-403.

[22] Murdock, H. J., De Bruijn, K. M., & Gersonius, B. (2018). Assessment of critical infrastructure resilience to flooding using a response curve approach. Sustainability, 10(10), 3470.

[23] Mao, Q., & Li, N. (2018). Assessment of the impact of interdependencies on the resilience of networked critical infrastructure systems. Natural hazards, 93(1), 315-337.

[24] Beheshtian, A., Donaghy, K. P., Gao, H. O., Safaie, S., & Geddes, R. (2018). Impacts and implications of climatic extremes for resilience planning of transportation energy: A case study of New York city. Journal of Cleaner Production, 174, 1299-1313.

[25] Aydin, N. Y., Duzgun, H. S., Wenzel, F., & Heinimann, H. R. (2018). Integration of stress testing with graph theory to assess the resilience of urban road networks under seismic hazards. Natural Hazards, 91(1), 37-68.

[26] Zhu, J., Manandhar, B., Truong, J., Ganapati, N. E., Pradhananga, N., Davidson, R. A., & Mostafavi, A. (2017). Assessment of infrastructure resilience in the 2015 Gorkha, Nepal, earthquake. Earthquake Spectra, 33(1), 147-165.

[27] Whitman, M. G., Barker, K., Johansson, J., & Darayi, M. (2017). Component importance for multi-commodity networks: Application in the Swedish railway. Computers & Industrial Engineering, 112 (October 2017), 274-288.

[28] Zhao, S., Liu, X., & Zhuo, Y. (2017). Hybrid Hidden Markov Models for resilience metrics in a dynamic infrastructure system. Reliability Engineering & System Safety, 164, 84-97.

[29] Fotouhi, H., Moryadee, S., & Miller-Hooks, E. (2017). Quantifying the resilience of an urban traffic-electric power coupled system. Reliability Engineering & System Safety, 163, 79-94.

[30] Panteli, M., Trakas, D. N., Mancarella, P., & Hatziargyriou, N. D. (2017). Power systems resilience assessment: Hardening and smart operational enhancement strategies. Proceedings of the IEEE, 105(7), 1202-1213.

[31] Kim, D. H., Eisenberg, D. A., Chun, Y. H., & Park, J. (2017). Network topology and resilience analysis of South Korean power grid. Physica A: Statistical Mechanics and its Applications, 465, 13-24.

[32] Cimellaro G.P., Tinebra A., Renschler C., Fragiadakis M. (2016). New Resilience Index for Urban Water Distribution Networks, Journal of Structural Engineering, 142 (8), C4015014

[33] Reed, D., Wang, S., Kapur, K., & Zheng, C. (2016). Systems-based approach to interdependent electric power delivery and telecommunications infrastructure resilience subject to weather-related hazards. Journal of Structural Engineering, 142(8), C4015011.

[34] Espinoza, S., Panteli, M., Mancarella, P., & Rudnick, H. (2016). Multi-phase assessment and adaptation of power systems resilience to natural hazards. Electric Power Systems Research, 136, 352-361.

[35] Hosseini, S., & Barker, K. (2016). Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports. Computers & Industrial Engineering, 93 (March 2016), 252-266.

[36] Labaka, L., Hernantes, J., & Sarriegi, J. M. (2016). A holistic framework for building critical infrastructure resilience. Technological Forecasting and Social Change, 103 (February 2016), 21-33.

[37] Chan, R., & Schofer, J. L. (2016). Measuring transportation system resilience: Response of rail transit to weather disruptions. Natural Hazards Review, 17(1), 05015004.

[38] Kim, H., Kim, C., & Chun, Y. (2016). Network reliability and resilience of rapid transit systems. The Professional Geographer, 68(1), 53-65.

[39] Kwasinski, A. (2016). Quantitative model and metrics of electrical grids' resilience evaluated at a power distribution level. Energies, 9(2), 93.

[40] Jonkeren, O., Azzini, I., Galbusera, L., Ntalampiras, S., & Giannopoulos, G. (2015). Analysis of critical infrastructure network failure in the European Union: a combined systems engineering and economic model. Networks and Spatial Economics, 15(2), 253-270.

[41] Testa, A. C., Furtado, M. N., & Alipour, A. (2015). Resilience of coastal transportation networks faced with extreme climatic events. Transportation Research Record, 2532(1), 29-36.

[42] Fang, Y., Pedroni, N., & Zio, E. (2015). Optimization of cascade-resilient electrical infrastructures and its validation by power flow modeling. Risk Analysis, 35(4), 594-607.

[43] Rochas, C., Kuzņecova, T., & Romagnoli, F. (2015). The concept of the system resilience within the infrastructure dimension: application to a Latvian case. Journal of Cleaner Production, 88(February 2015), 358-368.

[44] Verma, T., Araújo, N. A., & Herrmann, H. J. (2014). Revealing the structure of the world airline network. Scientific reports, 4(1), 1-6.

[45] Pant, R., Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2014). Stochastic measures of resilience and their application to container terminals. Computers & Industrial Engineering, 70, 183-194.

[46] MacKenzie, C. A., & Barker, K. (2013). Empirical data and regression analysis for estimation of infrastructure resilience with application to electric power outages. Journal of Infrastructure Systems, 19(1), 25-35.

[47] Omer, M., Mostashari, A., & Nilchiani, R. (2013). Assessing resilience in a regional road-based transportation network. International Journal of Industrial and Systems Engineering, 13(4), 389-408.

[48] Ouyang, M., Dueñas-Osorio, L., & Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. Structural safety, 36(May-July 2012), 23-31.

[49] Reed, D. A., Powell, M. D., & Westerman, J. M. (2010). Energy infrastructure damage analysis for hurricane Rita. Natural Hazards Review, 11(3), 102-109.

[50] Kajitani, Y., & Sagai, S. (2009). Modelling the interdependencies of critical infrastructures during natural disasters: a case of supply, communication and transportation infrastructures. International journal of critical infrastructures, 5(1-2), 38-50.

Appendix A. Overview of the reviewed articles

***Table* 10.** Overview of the 50 reviewed articles according to the eight overarching categorization aspects.

Ref	Infrastructures addressed		Inter-. dep.	Countries	Hazard	Approach	Methods	Improvements	Conclusion
	No.	Type							
[1]	1	Electricity	N	Netherlands	Heat wave, Flooding	M&S	Engineering	Analysed: Protection, Functional Capacity	Assessment
[2]	1	Metro	N	UK	NA	M&S	NW Top	Suggested: Protection, Structural Capacity, Functional Capacity	Indications
[3]	1	Road	N	USA	Flooding	M&S	System Dynamics	No suggestions	No conclusions
[4]	1	Maritime	N	USA	Earthquake	M&S	Probabilistic	Suggested: Structural Capacity, Functional Capacity	No conclusions
[5]	1	Air	N	Spain	NA	M&S	NW Flow, Statistical	Analysed: Functional Capacity, Organizational processes, Structural Capacity	No conclusions
[6]	2	Electricity, Gas	Y	USA	Hurricane	M&S	NW Flow, Probabilistic	Analysed	Assessment
[7]	1	District heating	N	Latvia	Extreme temperatures	M&S	Probabilistic	No suggestions	No conclusions
[8]	3	Water supply, Electricity, Gas	Y	Japan	Earthquake	Empirical	Statistical	No suggestions	Indications
[9]	2	Electricity, Metro	Y	USA	Hurricane	Empirical	Statistical	No suggestions	Comparisons
[10]	3	Railway, Electricity, SCADA	Y	Sweden	NA	M&S	NW Flow	No suggestions	No conclusions
[11]	3	Electricity, Railway, Road	Y	Australia	Heat wave	Empirical	Surveys, Expert elicitation	Suggested: Structural Capacity, Functional Capacity, Buffers - Dependencies	No conclusions
[12]	4	Electricity, Railway, Water supply, Road	N	Sweden	NA	Empirical	Statistical	No suggestions	Comparisons
[13]	1	Road	N	Nepal	Land slides, Earthquake	M&S	NW Top, Expert elicitation, Monte-Carlo	Suggested: Organizational processes	No conclusions
[14]	2	Electricity, Water supply	Y	Nepal	Earthquake	M&S	NW Top	No suggestions	Comparisons
[15]	4	Electricity, Water supply, Road, Shelter	Y	USA	Earthquake, Tsunami	M&S	Probabilistic, NW Top	Analysed: Retrofitting, Organizational increase, Alternative supply	Comparisons
[16]	13	Food supply, Fire & Rescue, Oil & Petroleum, Electricity, Road, Metro, Industry, Broadband (fibre), Banks, Business, Hospitals, Governmental Services, Water & Waste	Y	USA	Hurricane	M&S	Dynamic economic	Suggested: Protection, Functional Capacity, Buffers - Dependencies	Comparisons
[17]	2	Electricity, Metro	Y	UK	Flooding	M&S	NW Flow	No suggestions	No conclusions

Ref	Infrastructures addressed		Inter-. dep.	Countries	Hazard	Approach	Methods	Improvements	Conclusion
	No.	Type							
[18]	1	Road	N	Nepal	Land slides, Earthquake	M&S	NW Top, Expert elicitation	Suggested: Organizational processes	No conclusions
[19]	3	Electricity, Gas, Oil & Petroleum	Y	Canada	Hurricane, Flooding	M&S	NW Top, Probabilistic	Analysed: Organizational increase, Buffers - Resources	No conclusions
[20]	2	Waste water , Road	Y	China	Flooding	M&S	NW Flow	Suggested: Structural Capacity, Functional Capacity, Demand management	No conclusions
[21]	5	Electricity, Gas, Mobile, Fixed telephony, Water supply	N	USA, Japan, Chile, New Zealand, Mexico, Philippines, Algerie, Iran, Costa Rica, Peru, Turkey, Taiwan	Earthquake	Empirical	Statistical	No suggestions	Comparisons
[22]	5	Electricity, Road, Railway, Mobile, Fixed telephony	Y	Canada	Flooding	Expert	Expert elicitation, Surveys, Probabilistic	Analysed: Structural Capacity, Buffers - Resources, Protection	No conclusions
[23]	3	Electricity, Broadband (fibre), Water supply	Y	China	Typhoon	M&S	NW Top, NW Flow	Analysed: Buffers - Resources	No conclusions
[24]	2	Oil & Petroleum, Road	Y	USA	Climate change	M&S	NW Flow, Optimization	No suggestions	No conclusions
[25]	1	Road	N	Nepal	Earthquake	M&S	NW Top	No suggestions	Indications
[26]	2	Electricity, Water supply	N	Nepal	Earthquake	Empirical	Surveys	No suggestions	No conclusions
[27]	1	Railway	N	Sweden	NA	M&S	NW Flow, Optimization	No suggestions	Indications
[28]	1	Water supply	N	China	Intoxication	M&S	Probabilistic	Suggested: Buffers - Resources, Structural Capacity, Functional Capacity	No conclusions
[29]	2	Electricity, Road	Y	USA	NA	M&S	NW Top, Probabilistic	Suggested: Buffers - Resources, Organizational processes	Comparisons
[30]	1	Electricity	N	UK	Storm	M&S	Engineering, Monte-Carlo	Analysed: Structural Capacity, Organizational increase, Smart strategies	No conclusions
[31]	1	Electricity	N	South Korea	NA	M&S	NW Top	Suggested: Structural Capacity, Recovery timing	No conclusions
[32]	1	Water supply	N	Italy	Earthquake	Index	NW Flow	Analysed: Functional Capacity, Organizational processes	No conclusions
[33]	3	Electricity, Mobile, Fixed telephony	Y	USA	Hurricane	Empirical	Statistical	No suggestions	No conclusions

Ref	Infrastructures addressed		Inter-. dep.	Countries	Hazard	Approach	Methods	Improvements	Conclusion
	No.	Type							
[34]	1	Electricity	N	UK	Flooding, Storm	M&S	Probabilistic, NW Flow	Analysed: Protection, Structural Capacity, Organizational increase	Indications
[35]	1	Maritime	N	USA	NA	M&S	Probabilistic, Expert elicitation	No suggestions	No conclusions
[36]	2	Nuclear, Water supply	N	Spain	NA	Expert	Expert elicitation	Suggested: Organizational increase	Comparisons
[37]	1	Railway	N	USA	Hurricane, Snow storm	Empirical	Surveys, Statistical	Suggested: Protection, Structural Capacity	No conclusions
[38]	1	Metro	N	USA	NA	M&S	NW Flow	No suggestions	No conclusions
[39]	1	Electricity	N	USA	Earthquake, Hurricane	Empirical	Statistical	No suggestions	Indications
[40]	1	Electricity	N	Italy	NA	M&S	Dynamic economic	No suggestions	No conclusions
[41]	1	Road	N	USA	Storm surge	M&S	NW Top	No suggestions	No conclusions
[42]	1	Electricity	N	France	NA	M&S	NW Flow, Optimization, Engineering	Analysed: Structural Capacity	No conclusions
[43]	1	District heating	N	Latvia	Flooding	M&S	NW Top, Optimization	Suggested: Organizational processes	No conclusions
[44]	1	Air	N	Global	NA	M&S	NW Top	No suggestions	Assessment
[45]	1	Maritime	N	USA	NA	M&S	Discrete time model	No suggestions	No conclusions
[46]	1	Electricity	Y	USA	NA	Empirical	Statistical, Dynamic economic	No suggestions	No conclusions
[47]	1	Road	N	USA	NA	M&S	NW Flow	No suggestions	No conclusions
[48]	1	Electricity	N	USA	Hurricane, Random hazard	M&S	NW Top, Probabilistic	Analysed: Retrofitting, Monitoring, Structural Capacity	Assessment
[49]	1	Electricity	N	USA	Hurricane	Empirical	Statistical	Suggested: Structural Capacity	Assessment
[50]	6	Electricity, Gas, Water supply, Broadband (fibre), Fixed telephony, Road	Y	Japan	Earthquake	M&S	Surveys, Static economic, NW Flow	No suggestions	No conclusions

List of errata in PhD thesis

After the submission of the thesis on May 8, 2020, the following changes and additions have been implemented in the final printed and published version:

- On page x under 'List of appended papers', and on page 133 and page 165, a comment to Paper VI and Paper VII have been added:
    - Paper VI: "Article published online in Journal of Management of Engineering on July 9, 2020. Printed version published in Volume 36 Issue 5 – September 2020."
    - Paper VII: "Revised version of the manuscript submitted to Reliability Engineering & System Safety on July 8, 2020."
- Minor changes:
    - Heading and spacing in table on page xi ('IMPROVER-project publications) have been edited
    - Quotation mark removed from quotation on page 5 in the introduction and changed to italic font, to be consistent with the rest of the thesis.
    - In the third line in section 1.4 (Research objectives), "as presented on Table 1" has been changed to "as presented **in** Table 1".

Bjarte Rød

Tromsø, Norway
August 2020