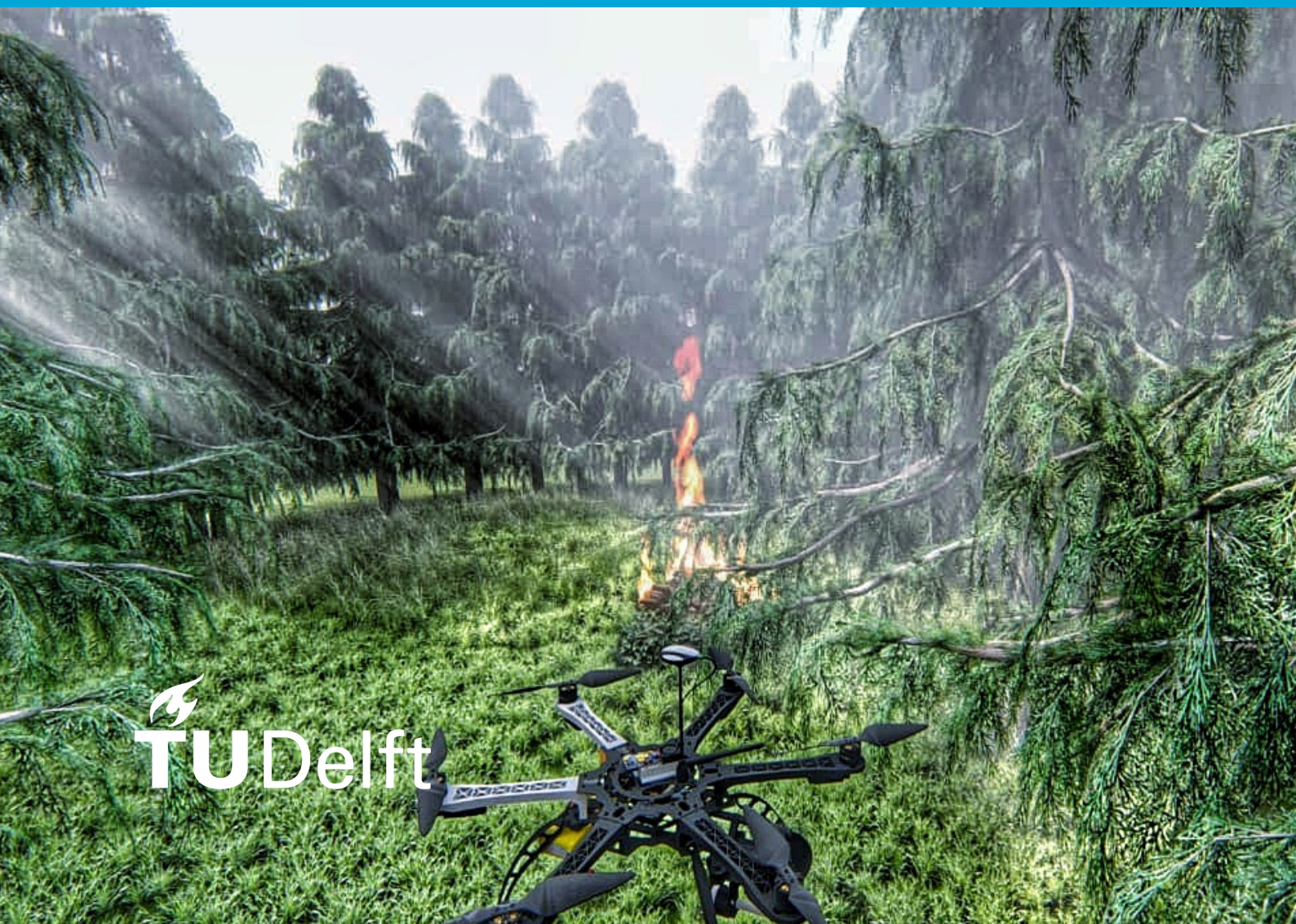
Assessing Cyber Security of Innovations in Climate Disaster Resilience

An Extension to the Test and Implementation Framework of the BRIGAID program

Sharwan A. Adjodha
Delft University of Technology



ASSESSING CYBER SECURITY OF INNOVATIONS FOR CLIMATE DISASTER RESILIENCE

A thesis submitted to the Delft University of Technology

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in **Engineering and Policy Analysis**

Faculty of Technology, Policy & Management

by

Sharwan Akaash Adjodha

Student number 4212843

To be defended publicly on October 2, 2019

Graduation committee

First supervisor:	Prof.dr.ir. P.H.A.J.M. van Gelder	TU Delft (TPM), Section RSS
Second supervisor:	Dr. S. Cunningham	TU Delft (TPM), Section PA
Advisor:	Dr. K. Labunets	TU Delft (TPM), Section O&G
External supervisor:	ir. J.R. Moll	BRIGAID, TU Delft (CEG)

Adjodha, S.A. (2019). *Assessing Cyber Security of Innovations for Climate Disaster Resilience* (Master's Thesis, Delft University of Technology, the Netherlands). Retrieved from `http://repository.tudelft.nl/`.

The work in this thesis was made in the:

Section of Safety and Security Science
Department of Values, Technology and Innovation
Faculty of Technology, Policy & Management
Delft University of Technology

BRIGAID Program
This project has received funding from the European Union's Horizon2020 research and innovation program under grant agreement No 700699.

COPYRIGHTS

This document was typeset using LaTeX. The document layout was generated using the `arsclassica` package by Lorenzo Pantieri, which is an adaption of the original `classicthesis` package from André Miede. Further alterations were made by the author.

PREFACE

This thesis is the concluding fulfillment of the requirements for the degree of Master of Science in Engineering and Policy Analysis. As my academic career comes to an end, I can look back at seven remarkable years. My time here in Delft, as prolonged as it has been, gave me some great memories, friends, and accomplishments. This partial fulfillment served as the final test of my academic skills, and I joyfully present the resulting product.

The research presented in this thesis is commissioned by the Safety and Security Science section of the Technology, Policy, and Management faculty at Delft University of Technology and BRIGAID. BRIGAID is a four-year program (2016-2020) under the EU Horizon2020 program aimed to effectively bridge the gap between innovators and end-users in resilience to floods, droughts, and extreme weather. The research addresses the importance of cybersecurity for innovation projects. With this thesis, I hope to contribute to the knowledge of cybersecurity in innovation and provide BRIGAID with an adequate extension to their assessment tool. The topic of cybersecurity runs like a thread through my Master's program for the past two years. It served as the main topic of several projects in my first year, as well as during my semester abroad in the Fall of 2018 at Indiana University Bloomington in the United States. Besides becoming a Hoosier, I studied the federal budgeting of cybersecurity in the US. It showed the increased awareness and importance of this topic and inspired me in pursuing a thesis subject concerning cybersecurity.

This thesis is an individual project. However, numerous people have supported me in reaching this result. Firstly, I want to thank dr. Kate Labunets, who sits in my committee as the advisor. She was more than my advisor; she supervised my work in detail and got the best out of me. From the start, I could sense the honesty in her comments and the commitment to guide me, and it is very much appreciated. Her expertise in this subject has significantly improved the level of detail in this thesis. Secondly, the chair of the committee, Prof.dr.ir. Pieter van Gelder. Prof. van Gelder was always willing to aid me in improving my work with critical yet fair comments. Thirdly, dr. Scott Cunningham and I knew each other from earlier in the Engineering and Policy Analysis program. During my stay in the US, I already contacted dr. Cunningham because I knew he would be of great support during my thesis. Lastly, ir. Roelof Moll, who is the project manager of BRIGAID. From the start, Roelof was very interested in my research and supported in every way he could, with the information he provided and detailed knowledge on the project. He also established contact with various innovators. The innovators and experts deserve recognition for their help and willingness to provide me with information on their projects.

I want to conclude with my gratitude towards my friends and family. Especially my parents and sister, who had to put up with a by times stressed-out student. The support of friends, family, and study companions have made this process easier with some much-needed moments of relief and leisure.

I appreciate you all, enjoy the read!

Sharwan Adjodha
Delft, October 2019

EXECUTIVE SUMMARY

In the coming decades, more frequent and more extensive climate disasters such as coastal and river floods, droughts, extreme weather, and wildfires can be expected worldwide. Various literature suggests that these natural hazards are occurring more frequent and more extensive due to climate change. In combination with climate change comes an anticipated increase in population, resulting in more people getting exposed to an increasing number of climate-related hazards. Hazard mitigation and climate adaptation strategies are necessary to decrease the vulnerability of society. However, the substantial economic costs of risk mitigation create a trade-off for decision-makers in the political arena, making this a socio-political dilemma. Both direct and indirect effects are affecting the impact of climate disasters on society. Innovations will be required to face this grand challenge. Both local and global innovation initiatives create new standard practices in climate adaptation strategies, which benefit the safety of society from natural disasters.

With the use of innovations, new challenges arise. Innovations often come with the introduction of new technology or technological development of current systems. Challenges involve the threats to the system from a new dimension, the cyberspace. Cybersecurity is used to protect the cyberspace in which systems operate. The developing use of modern communication and information technology in a broader range of systems raises the need for secure cyberspace. In the case of innovation, cybersecurity becomes increasingly important. We must consider the trade-off between the security of the cyberspace and innovation freedom when addressing the cybersecurity of innovation projects.

The BRIGAID program is part of the EU's H2020 initiative to stimulate innovation. The program developed a methodology consisting of a Test and Implementation Framework (TIF) and a set of practical tools. Throughout the development of innovation projects concerning climate disaster resilience, BRIGAIDs tools are offered to support efficient development and market introduction of promising innovations. The methodology in its present state still requires an extension to cover cybersecurity issues. It should be assessed where and whether cybersecurity is relevant within the TIF, and how this can be included in the framework.

The objective of this study is to identify key cyber components of innovation projects. We assess where cybersecurity is relevant within innovation and find an a risk assessment approach. The final objective is to develop an extension to the TIF in which cyber threats are effectively identified and mitigated. The following main research question is posed to reach the objectives:

How can cybersecurity threats be effectively identified and mitigated to minimize the risk of cyber attacks on innovation projects for climate disaster resilience?

This research defines key cyber components and establishes an assessment for the cybersecurity readiness as an extension to BRIGAIDs TIF self-assessment tool. We compile a list of cyber components with a literature review on components in related fields of study. We validate the list with semi-structured interviews among cybersecurity and innovation experts. We determine key cyber components for innovation projects by surveying innovators. We also use the survey results to gather data from the innovators on their perception of cybersecurity and the cyber components of their projects' systems. We use the results to identify representative cases for the risk assessments.

For the structure of the risk assessment, we find the case study to be most fitting due to the exploratory nature of the research and innovation projects in climate disaster resilience. We de-

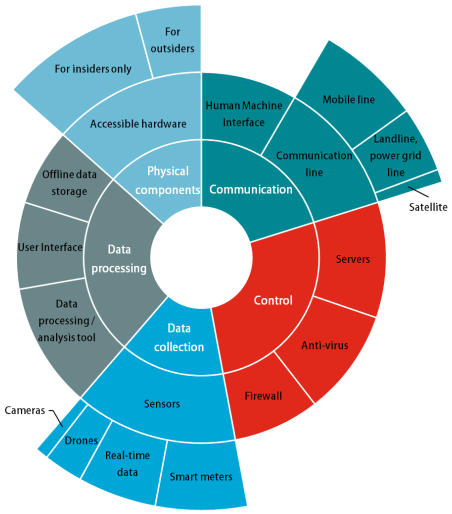


Figure 0.1: The identified key cyber components for innovation projects

fine the cases as unique innovation projects with key cyber components that will be subjected to risk management. We use data from interviews, the project database, and the survey for the assessments. After a thorough literature review, we found the SecRAM methodology most fitting to the needs of this study. We use this method for the risk assessments, and eventually to help design the extension of the TIF of BRIGAID.

Innovations projects have unique elements which define and distinguish them from other types of projects. From the literature review we compile a framework with four elements that form an innovation project. The freedom of innovation was found to be essential and unique to innovation. The freedom to work in a system and improve it is an crucial trade-off with the security of that system. The human factor and human interactions within a system merge into the roles and responsibilities element. The cyber part of innovation is covered by the information architecture element, while the physical security element covers the physical side of the system. Within those last two elements, we identify the space for cyber components. Cyber components are parts of the cyber-physical system of innovation projects. We categorize the components into five elements, namely components of communication, control, data collection, and data processing, and physical components. The data from the expert interviews present different perspectives to assess the cybersecurity of systems. We find key cyber components for innovations by using the results from the innovators' survey and compare the most occurring components to the results from the expert interview. Figure 0.1 presents the identified key cyber components for innovation projects.

We sought a case with a high perceived importance of cybersecurity and one satisfied with the project's current cybersecurity efforts. We identified GM4W and QoAir as representative innovation projects for the case studies. First, we subjected the GM4W system to a risk assessment. The system's main data transmission was GNSS data. High-risk threats were jamming and spoofing of signals, failure of hardware, theft, insider attack, human errors, and power outage. Some of these threats have similar mitigation measures. The most important measures are data encryption, preparing a backup protocol, creating a robust network, prioritize critical assets, and integrity monitoring. Second, we had a risk assessment of QoAir. The system's main data transmission here was sensor data through a blockchain infrastructure. Theft or failure of hardware components is a high-risk to this system, along with software failure. We found two of risk treatment controls in this assessment with a robust network and backup protocols.

The cross-case synthesis compared the threats to both systems, and we distinguished three types of threats from this comparison, namely hardware-related, software-related, and human-related threats. We compared the risk treatment controls as well. Creating a robust network and having backup protocols are controls identified in both assessments and general good practices for risk treatment. Data encryption, integrity monitoring, staff training, and identity and access control are controls for software- and human-related threats more specific to a system similar to GM4W. We use the results of the risk assessment to make recommendations for innovation projects and to design the cybersecurity assessment extension for the TIF tool.

The TIF analyzes climate adaptation innovation projects as socio-technical systems. From this type of system, we derive three assessments, namely technical testing, impact assessment, and social testing. Each assessment category works independently. With creating the extension, we must choose between extending one of the categories and creating a new sheet for cybersecurity. Adding cybersecurity to an existing category means that cybersecurity must have significant overlap with the category's current perform. Current assessment questions consider the safety of the system. The assessment tool addresses technical, environmental, and societal concerns on safety. However, the security of the system itself is out of the scope of the current tool.

Therefore, we choose to design a separate sheet for cybersecurity, making it a new category in the TIF tool. Having a different category makes our extension a standalone assessment tool within the TIF for the security of information and services as provided by innovations (see Figure 0.2). The characteristics of assets, confidentiality, integrity, and availability are central in the SecRAM risk assessment. Assets of systems are assessed based on the presence of these characteristics. We structure the new cybersecurity assessment by dividing the scoring into three subcategories, each covering one of the CIA characteristics. In this design, each of the three CIA characteristics represents a Performance Index for cybersecurity.

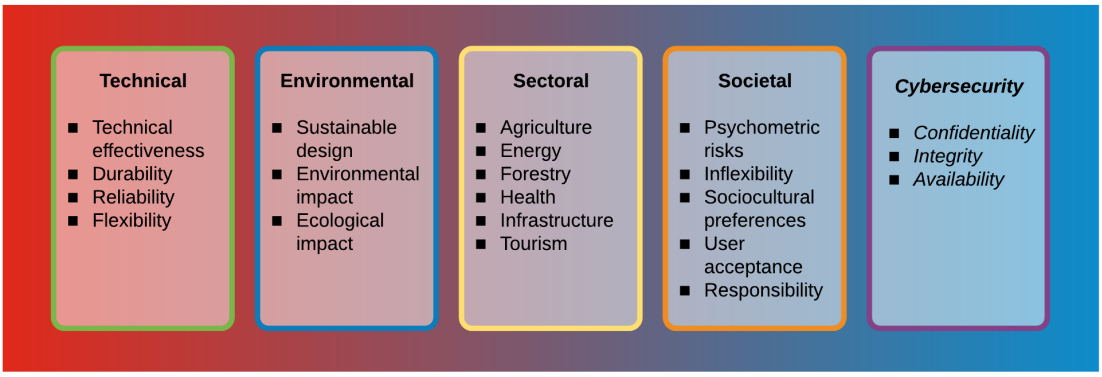


Figure 0.2: TIF extension design for cybersecurity

We find that the identified key cyber components for innovation projects benefit the identification and mitigation of cyber threats. When assessing an innovation, the cyber components serve as a starting point of the assessment. We used SecRAM as the risk assessment method in this study and aimed to test whether the method applies to the risk assessment of innovation projects. We conclude that the SecRAM method serves its purpose and applies to the innovation projects in the context of this study. The risk assessments applied to different cases with contrasting structures and enabled us to identify and mitigate cyber threats effectively.

The cases in this study revealed numerous potential threats for innovation projects in climate disaster resilience. We categorize the threats to hardware-, software-, and human-related threats. We found mitigation controls for each category, and in general terms as well. Creating a robust network and having backup protocols are controls identified in both assessments and general good practices for risk treatment. These mitigation controls apply to most of the identified risks for innovation projects.

The TIF cybersecurity extension from this study is verified and validated to be of use in the current state. The extension follows the same structure as the rest of the tool and works as a standalone assessment. We recommend BRIGAIDs experts to critically reflect on the tool and determine whether the extension improves the overall tool enough to be implemented. For the validation, we use the Technology Acceptance Model (TAM) for the implementation of the proposed cybersecurity extension. The TAM aims to measure the usefulness and ease of use as perceived by the intended users. The model gives an indication of the intention to use and eventual usage of the new technology. In this study, we applied to the model to the perceptions of BRIGAIDs Project Manager. We recommend applying this validation model to a sample of innovators and partners of BRIGAID to determine their viewpoints on the extension of the tool. Both the expert validation and intention to use the model help indicate whether the extension is worth implementing.

We recommend innovators to self-assess their systems with the proposed tool extension. The tool benefits innovators in different stages of development. Addressing issues with the system early in the development cycle serves the project by exposing threats right away and limiting the number of unaddressed risks later on in the cycle. The current tool directs innovators to assess the project focused on the implication to the environment and the climate disaster that they address. The extension forces innovators to evaluate their projects systematically. This different perspective conceptualizes the data flows and infrastructure within the system and can bring new insights to the innovation.

For future research, we address the methodology in this study. We used a mix of both quantitative and qualitative methods. The use of numerous methods had the benefit of providing different results that apply to different parts of the study. For example, we used a literature review, expert interviews, and a survey among innovators to compile the list of key cyber components. Each method provided us with information from different perspectives. However, we found the use of a mix of methods to be challenging, especially when structuring the gained data and scientifically using that data. Each method comes with its assumptions and limitations, and by drawing conclusions from different sources, we should address the combination of assumptions and limitations as well to ensure the validity of our conclusions.

Finally, the applicability of the risk assessment method used in this study is the main takeaway of this study. The applicability of SecRAM needed testing in new fields of study, and we conclude that the method applies to the assessment of innovation projects. We base this conclusion on a small sample size, and future research should expand upon the range of projects assessed following the SecRAM method. Involving the innovators and experts in the data-gathering phase, as we did in this study is recommended. However, the innovators' involvement could be extended to the assessment phase as well. This involvement is not addressed in this study but should be considered for future research.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ATM Air Traffic Management . . . 42
BNs Bayesian Networks . . . 38
BRIGAID **BRI**dge the **GA**p for **I**nnovations in **D**isaster resilience . . . 25
CIW Climate Innovation Window . . . 27
EU European Union . . . 25
CIA confidentiality, integrity, and availability . . . 11
GNSS Global Navigation Satellite Systems . . . 30
H2020 Horizon2020 . . . 25
HMI human machine interface . . . 15
HVAC Heating, ventilation, and air conditioning . . . 16
IoT Internet of Things . . . 9
ISO International Standards Organization . . . 35
MMU malfunction management unit . . . 16
NIST National Insitute of Standards and Technology . . . 35
PA Primary Asset . . . 43
RFD Research Flow Diagram . . . 7
RINA recursive internetwork architecture . . . 42
SA Supporting Asset . . . 43
SCADA Supervisory Control And Data Acquisition . . . 9
SecRAM Security Risk Assessment Methodology . . . 42
TAM Technology Acceptance Model . . . 70
TIF Test and Implementation Framework . . . xiv
TRL Technical Readiness Level . . . 25
UHI Urban Heat Island . . . 31

1 INTRODUCTION

1.1 RESEARCH CONTEXT

1.1.1 Climate Disaster Resilience

In the coming decades, more frequent and more extensive climate disasters such as coastal and river floods, droughts, extreme weather, and wildfires can be expected worldwide. Various literature suggests that these natural hazards are occurring more frequent and more extensive due to climate change (Anderson and Bausch, 2006; Van Aalst, 2006; Blöschl et al., 2017). In combination with climate change comes an expected increase in population, resulting in more people getting exposed to an increasing amount of weather-related hazards (Forzieri et al., 2017). Among those hazards, heat waves are found to be one of the most prominent and deadly hazards. The increase in frequency and impact is predicted for southern Europe (Rohat et al., 2019). The forecasted increase in climate disasters should be addressed to prepare the population better and minimize their exposure and vulnerability to these disasters. Wilhelmi and Hayden (2010) discuss how hazard mitigation and climate adaptation strategies, among other elements in their framework, address the vulnerability of the population. Lowering the vulnerability of the population is directly attainable by reducing the risk of a climate disaster. However, the high economic costs of risk mitigation create a trade-off for decision-makers, making this a socio-political dilemma (Jonkman et al., 2005). The investment that must be made to reduce the risks are expensive, yet crucial to protect inhabitants from casualties and significant material damage. These direct effects are not the only way populations can be vulnerable to climate disasters. Indirect effects, such as effects on the economy or critical infrastructures, should be addressed as well (Wilhelmi and Hayden, 2010).

Forzieri et al. (2018) found the predicted increase in damage from climate disasters to be especially significant when addressing climate disaster resilience of critical infrastructure. The increasing interconnectedness of these infrastructures makes damages more impactful, and climate change resilience is therefore encouraged. Addressing forecasts and future scenarios have brought out key aspects that differ from other studies. Leichenko (2011) identified key aspects of hazard resilience, including innovation. Different studies find innovation as a requirement for adaptation to climate-related disasters (Pelling, 2010; Olwig, 2012). Innovations can benefit the adaptation process both locally and globally. Pelling (2010) explains this with (global) common practices that are created by (local) individuals with innovative ideas. The innovation spreads and becomes the norm as peers copy the idea. The use of innovative ideas in climate disaster resilience locally can be used by others and therefore benefit the global population.

With the use of innovations, new challenges arise. Innovations often come with the introduction of new technology or technological development of current systems. These emerging technologies expose systems to new challenges for their technology and risk assessment (Hellström, 2003). Challenges involve the threats to the system from a new dimension, the cyberspace. Cybersecurity is used to protect the cyberspace in which systems operate Craigen et al. (2014). The developing use of new communication and information technology in a broader range of systems raises the need for secure cyberspace. In the case of innovation, cybersecurity becomes increasingly important. Hart et al. (2014) discuss the issue of cybersecurity and the necessity of openness and liberty to allow for innovation. We must consider the

trade-off between the security of the cyberspace and innovation freedom when addressing the cybersecurity of innovation projects.

1.1.2 BRIGAID Program

Innovations will be required to face the grand challenge of climate disaster resilience. Within the European H2020 program BRIGAID, a methodology is being developed to assess technical and societal acceptance, and market readiness of innovations for climate disaster resilience. The program supports faster and more effective development and market introduction of promising innovations. BRIGAID aims to become the quality label for the development of innovations for climate adaption and risk reduction from climate-related disaster impacts in Europe and beyond. The projects are currently all in Europe since the group falls under the European Commission. The goal of BRIGAID, however, is to benefit the global population eventually (BRIGAID, 2016a). Kahn (2005) found that wealthier regions suffer less damage from the same amount and severity of natural disasters when compared to poor regions. The comparison reveals that, besides geographical location, institutions play a role in natural disaster resilience. European innovations can eventually be adjusted for other regions and used there for climate adaptation as well.

The BRIGAID methodology consists of a TIF and a set of practical tools, designed to help an innovator moving his innovation forward, but also to support the end-user defining his requirements for the acceptance of innovations. The TIF tool addresses the challenges for innovators in the climate adaptation innovation process and seeks to bridge the gap between innovators and end-users (see Figure 1.1). The methodology in its present state still requires an extension to cover cybersecurity issues. It should be assessed where and whether cybersecurity is relevant within the TIF, and how this can be included in the framework. Cybersecurity readiness should be an indicator to innovators on their ability to identify and mitigate cybersecurity threats to minimize the risk of cyberattacks on their innovation projects.

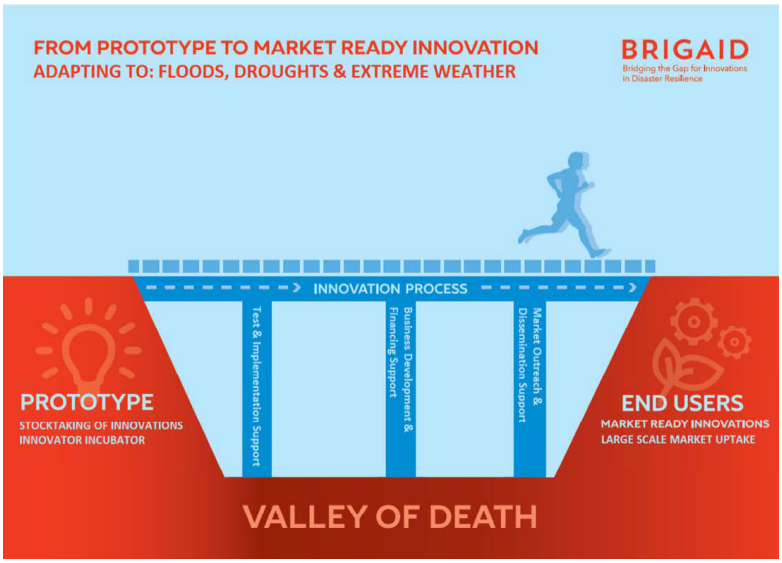


Figure 1.1: "Bridge across the Valley of Death" (Sebastian et al., 2019b, p.3)

1.2 PROBLEM DEFINITION

1.2.1 Research Scope

Cybersecurity is a relatively new concept in the scientific field. Even though many years of research have passed, there are still concerns about how to cope with cybersecurity threats. Singer and Friedman (2014) address this concern with the example of CIA director General Michael Hayden, who is quoted saying that he had meetings with colleagues in Washington

D.C. in which there was no clear picture of the long-term implications of their decisions on addressing cybersecurity. The CIA director stated that they were unable to make sound decisions because of this lack of knowledge. To put it in the words of the authors: "In short, no issue has emerged so rapidly in importance as cybersecurity. And yet there is no issue so poorly understood as this 'cyber stuff'" (Singer and Friedman, 2014, p.4).

Refsdal et al. (2015) define cybersecurity as the protection against cyber-threats of cyber-systems. Cyber threats are any threat that comes from the cyberspace. The authors emphasize the role of the cyber-threats in this definition. Cybersecurity is not defined by what needs to be protected, but more so on the kinds of threats to the assets that need protection. The definition is one of the differences between cybersecurity and information security. Although information assets may often be targets of cyber threats, not all information targets can be attacked through the cyberspace, and therefore do not fall under the protection of cybersecurity (Refsdal et al., 2015). Von Solms and Van Niekerk (2013) argued for this difference of concepts stating that cybersecurity includes more components than traditional information security. Cybersecurity does not solely protect information sources but goes beyond that and also covers other components such as the human factors within a system. The role of humans is important in cybersecurity, because of the potential targeting of humans and (unknowingly) participation of humans in cyber attacks.

Van de Ven (1986) defines innovation as a new idea, which could come from numerous sources, such as a recombination of old ideas, a challenge to the existing order, a formula, or a unique approach as perceived by the people involved. The latter may lead to the idea of being an 'imitation' of an existing idea and still be defined as an innovation (Van de Ven, 1986). The relevancy of innovations lays within its role to the dynamics of economic growth and socio-economic development. We deem innovations as essential when it comes to economic growth and sustainability agendas worldwide (Edwards-Schachter, 2018). Vargas-Hernández et al. (2010) define innovations as the main source of economic growth, with new employment opportunities and environmental benefits following from that growth.

In the case of innovation projects, cybersecurity plays a significant role. Radanliev et al. (2018) argue the role of cybersecurity to be increasingly important due to the ongoing technological development and the increase in both the number and severity of cyberattacks. Technological innovations have led to rapidly changing environments of systems with risks that are relatively new and therefore, difficult to control and foresee. Creating the right mitigation strategy for these risks can reduce them to a manageable level (Abdel-Basset et al., 2019).

As mentioned in Section 1.1.2, BRIGAID's goal is to estimate the level of security of the innovation projects involved in the program. The goal of this study is to identify risks of climate adaptation innovation and assess whether the innovation projects have their systems prepared for such risks. The innovation projects affiliated with the BRIGAID program cover innovation projects specific intended to address climate disaster resilience efforts. This study focuses on innovation projects in general and aims to provide conclusions that are applicable to a wider range of subjects. The TIF tool of BRIGAID, however, is focused on the climate disaster resilience innovation. The intended improvements of this framework from this study should therefore be specific to this type of innovation as well.

Methodologically, we seek a risk assessment method that can assess projects in all phases of development, from early development to market implementation. Also, various literature classifies assessment methods by qualitative vs. quantitative analysis (Fabian et al., 2010; Patel et al., 2008; Cherdantseva et al., 2016). Where qualitative methods often use measures for security, such as low to high, quantitative methods attempt to measure risk numerically. Verendel (2009) argues that quantifying security limits the validity of the results of a methodology due to the lack of empirical data. Cherdantseva et al. (2016) also address the difficulty in finding historical system data and the lack of objective data at all. Subjective data, which qualitative analysis uses, can be collected more effective and more specific to the subject at hand. By

choosing a qualitative analysis, we try to find results that are, even though not as specific as numerical values, backed by reliable information specific to the subject.

1.2.2 Research Objectives

Based on the background and knowledge gaps found in the previous section, we introduce research objectives. These objectives clearly define the problem, from which we derive the problem questions. The three research objectives are as follows:

1. Identify key cyber components of systems of innovation projects
2. Assess where cybersecurity is relevant within innovation projects and select a risk assessment approach which can fill the lack of information on cyber threat mitigation
3. Develop an extension to the TIF in which the cybersecurity threats can be identified and mitigated effectively

1.2.3 Research Questions

The research objectives show how this study aims to tackle the problem at hand. The main question covering the objectives should address the identification and mitigation of cybersecurity threats in light of innovations. In this study, we focus specifically on innovations for climate disaster resilience, as featured in the BRIGAID program. The objectives lead to the following main research question:

How can cybersecurity threats be effectively identified and mitigated to minimize the risk of cyber attacks on innovation projects for climate disaster resilience?

The main research question can be broken down into several sub-research questions (SQs). The answering of the main research question is a stepwise process by answering each of the following sub-questions:

1. *What type of cyber components can be distinguished when assessing risks in innovation projects?*
   The first sub-question aims to come up with a specific set of components that are significant when assessing risks in innovation. We consider other fields of study with technological development as the main driver when compiling the list of components.
2. *What innovation projects within the BRIGAID project can provide the broadest variety of cyber components?*
   The the portfolio of BRIGAID introduces a wide variety of innovation projects. The projects are different in terms of climate disaster addressed, size, and readiness level, among other specifications. The purpose of this sub-question is to identify innovation projects that we consider representative examples of innovation projects in climate disaster resilience.
3. *What type of cyber risk assessment methods are applicable to risk assessment of innovation projects?*
   The purpose of this sub-question is to find a method to identify and mitigate risks effectively. The method used in this study should not only apply to the innovation projects of BRIGAID but innovation projects in general as well.
4. *Where can cyber risk management be of importance in the TIF of BRIGAID?*
   The TIF is the self-assessment tool of BRIGAID. There are various ways to extend this tool and improve it. The sub-question aims to explore all options and find the most effective result according to the findings of this study.
5. *What recommendations can be made based on the risk assessment of innovation projects for climate disaster resilience?*

The purpose of this sub-question is to reflect on the results of this study and identify key components and best strategies to effectively secure innovation projects from cyber threats.

The next section discusses the methodology and tools that we use to answer the research questions at hand.

1.3 RESEARCH METHODOLOGY

From the problem definition section, we derive a research plan designed to accomplish the objectives of this study. This section discusses the research approach and methodologies, which we use to answer the research questions. The approach consists of a mix of both quantitative and qualitative methods. The use of this mix of methods benefits the analysis, interpretation of findings, and reflection of the study (Galletta, 2013). Sale et al. (2002) found a strength of using mixed-methods research that quantitative and qualitative methods study the phenomenon subject to research from different points of view. Figure 1.2 presents an overview of the used methods in this study and main takeaways, specified to the sub-question(s) for which we use the method.

1.3.1 Context Establishment

The first sub-question aims to compose a list of cyber components that are significant to the risk assessment of innovation projects. We use several methods to compile the list of cyber components. First, we use a literature review for two reasons, to establish the context in which the cyber components are relevant to the assessed system and to find cyber components in related fields of study, similar to the systems of innovation projects as mentioned in this study.

Second, we use interviews with experts as a validation tool. The interviews are semi-structured to create space for reciprocity with the interviewees to clarify information and reflect on the discussed topics. Galletta (2013) found that semi-structured interviews make interviewees engage more with the topic and allows for this reciprocity. The information can be used later on in the study to validate results from the literature review and survey. We analyze the results from these interviews according to a deductive approach. The deductive approach starts with a theme or theory determined before the analysis (Zhang and Wildemuth, 2009). In this case, the list of cyber components is the starting point of the analysis. We gather the acquired data from the interviews to validate this list.

Third, we use a survey to gather information from innovators affiliated with the BRIGAID program. The survey provides the study with both quantitative data on the cyber components and qualitative data on the innovators' perception of the importance of cybersecurity in their innovation project and their satisfaction with current cybersecurity efforts. The results serve as an insight into the use of the cyber components in innovation projects.

1.3.2 The BRIGAID Case Study

For the second sub-question, we select representative cases based on the cyber components within the projects' systems. Therefore, we need to analyze the innovation projects within BRIGAID before we can make a grounded decision on what innovation projects we consider as representative. We use the survey results from the previous subsection to find representative innovation projects. Each innovation project affiliated with BRIGAID has its page on the Climate Innovation Window (CIW), BRIGAIDs informative webpage. We gather qualitative data and descriptive statistics of the innovation projects from the web content. We use the results from the survey and the data from the CIW to select the cases for this study.

The answer to the third sub-question leads us to a risk assessment method. We analyze the representative cases of innovation projects, and we apply the case study method to structure the research. We work with cases in this study to make generalizable conclusions for the cybersecurity of innovation projects. The cases are subject to a risk assessment. We use the results

of the assessment as a foundation for the recommendations made in this study. We choose the risk assessment methodology based on a literature review of the available methodologies in scientific literature and practice. The case study adopts the approach most effective when assessing innovation projects. The stepwise approach by Yin (2011) designs the case study in this research and is explained in greater detail in Section 4.1.

The fourth sub-question of the study involves the extension to the TIF of BRIGAID. Where the case studies address the research objective concerning the relevancy of cybersecurity in innovation projects, the tool extension satisfies the second objective of creating an extension for cyber threat identification and mitigation. We analyze the tool before commencing with the case study and re-evaluate after. We identify the potential slots within the tool for our extension with this re-evaluation. The case study database, filled with all the gathered data for our case studies, is used to create a self-assessment questionnaire with a scoring mechanism for the cybersecurity of an innovation project.

The fifth and final sub-question is a reflection on the results from the previous questions. We use the results from the context establishment and risk assessments to compile generalizable conclusions for innovations in a broader range of systems.

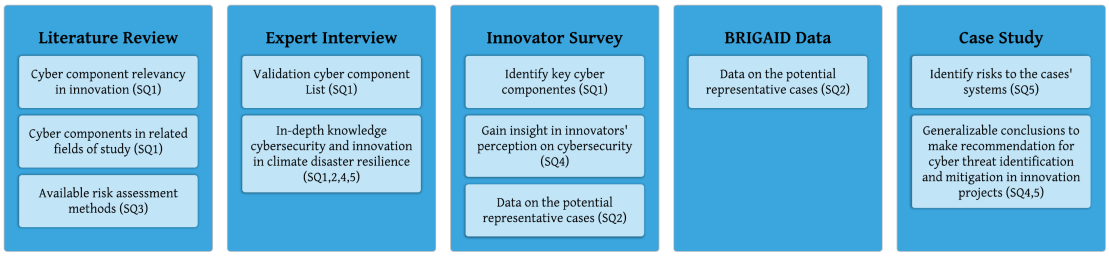


Figure 1.2: Research Methods

1.3.3 Data Collection

Yin (2011) addresses a key feature of case studies, which is requiring a large variety of data as input. We use several sources of information in this study. We consult both quantitative and qualitative data sources to acquire data. The primary source of data is scientific literature. We use scientific literature for the research on cyber components in innovation projects and the selection of a risk assessment method. Two reviewing methods structure the review, namely database searching and backward snowballing. The database search uses two repositories, Scopus and IEEE Xplore. The backward snowballing technique also includes other repositories, such as the TU Delft Repository and Google Scholar. Mendeley, which serves as a library for our sources, stores reviewed literature.

The second source of data is qualitative data from interviews. We use expert interviews for validation and data gathering. A semi-structured interview serves both needs and enriches the research with knowledge from both the academic and business perspective by having interviewees from both fields. We also design a survey for both quantitative data on the cyber components within the systems of BRIGAIDs innovation projects and qualitative data on the innovators' perception on cybersecurity of innovation. The results of the survey also indicate what innovation projects serve as representative cases for this study.

Lastly, we have archival data from BRIGAID and the projects involved. BRIGAID has an online database known as the Climate Innovation Window. This website contains data on all the innovation projects that were, or still are, involved in the BRIGAID program. We gather data on the innovation projects to gain knowledge on the selection of projects at our disposal and as input data for the risk assessments in the case studies.

1.3.4 Research Flow Diagram

Figure 1.3 shows the Research Flow Diagram (RFD) of this study. The RFD divides the research into four phases. Phase one is the introduction. In this phase, we introduce the research with its problem statement, research questions, and methodology. This phase translates to the first chapter of the report.

Phase two represents the desk research phase. In this phase, most of the literature review is conducted to gather information and input for the analyses. Firstly, we discuss the conceptualization of cyber components. The unique aspects of innovation projects are the main focus in this part of the study. We assess studies on innovation and related fields of study. The goal is to come up with a list of cyber components specifically for innovations. Secondly, the BRIGAID projects are analyzed and categorized according to the found cyber components. A database reports the projects, and a survey sheds light on the composition of projects within BRIGAIDs portfolio. Thirdly in this phase, the risk assessment methodologies available in the scientific literature are reviewed, and the next phase uses the method most fitting to the innovation projects.

Phase three is the case study, where we perform risk assessments on the selected projects. The methodology, as explained in the third step of phase two, also determines the type of case study that we use. The risk assessments result in cyber threat estimations for the individual cases, but the assessments deter generalized conclusion as well. The TIF tool of BRIGAID uses these generalized conclusions. The final step of phase three presents various options with recommendation and advice on the decision-making for these options. Phase four discusses the results from the previous phase. This phase is the concluding phase of this research, in which we present the conclusion of the study, discuss these conclusions, and recommend next steps and propose future research.

1.4 SIGNIFICANCE OF THE STUDY

We aim with this study to benefit to the understanding of the relevancy and significance of cybersecurity in society. The increasing use of the cyberspace and connectivity of society has raised numerous concerns about our safety, security, and privacy. Many studies focus on the concept of cybersecurity and how to govern this phenomenon adequately. We hope to benefit these findings by specifically addressing the cybersecurity of innovation. The BRIGAID program aids innovators in developing their projects more effectively. The use of BRIGAIDs tools benefits the innovators by making them reflect critically on their projects and the benefits to society and climate adaptation. This study addresses the found gap in the assessment tools for addressing the cyberspace and security of the projects' systems. The results of this study should aid BRIGAID in improving the TIF by extending the tool with a cybersecurity section, subsequently benefiting the innovations in their development.

1.5 THESIS OUTLINE

The structure of this report follows the research flow diagram, as presented in Section 1.3.4. After the introduction of the study in Chapter 1, the thesis continues with the definition and identification of cyber components for innovation projects (Chapter 2). Following the set of cyber components, Chapter 3 provides insight into the BRIGAID program and the innovation projects within its portfolio. The chapter concludes with the selected projects for the case study. Chapter 4 elaborates on the research methodology by conceptualizing risk management and narrow it down to a specific method for the risk assessment of innovation projects. Next, we present the results of the case study in Chapter 5. The results are further used to construct the cybersecurity extension of the TIF (Chapter 6). Lastly, the thesis wraps up with the conclusions of the study and a reflection on the findings, methods used, and relevance of the study, including recommendations for future research in Chapter 7.

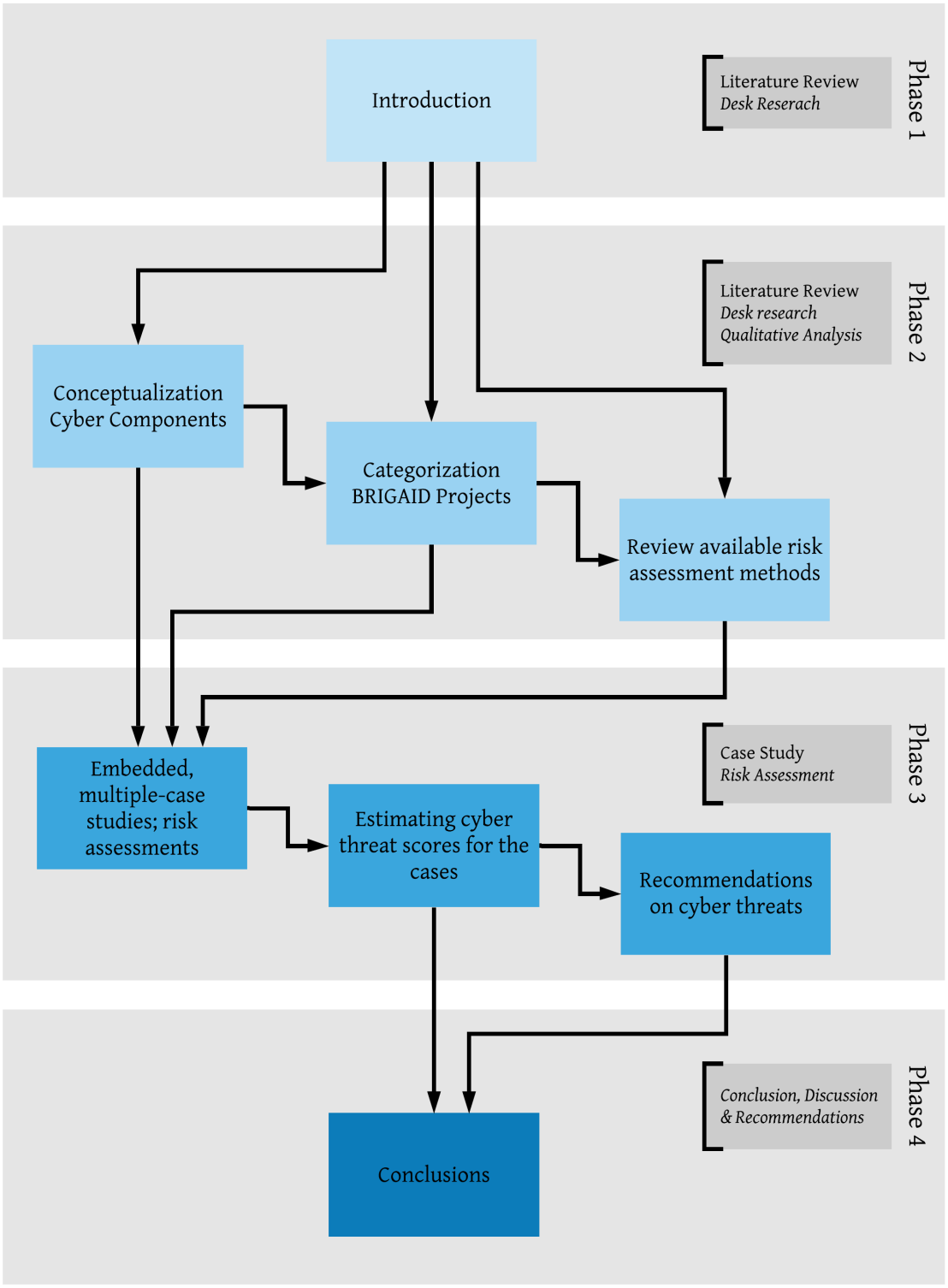


Figure 1.3: Research Flow Diagram

2 CYBER COMPONENTS

This chapter answers the first subquestion: What type of cyber components can be distinguished when assessing risks in innovation projects? Innovation projects have certain unique elements to them. Section 2.1 provides an overview of these elements. Section 2.1.1 discusses these elements as found in literature in related fields of study to innovation projects, such as smart cities and Internet of Things (IoT). Further subsections (Section 2.1.2 through Section 2.1.5) discusses each identified element. From these elements, we define cyber components. Section 2.2 touches on how we found these components and what their definition is. We validate the found cyber components through expert validation and an innovator survey. Section 2.3 discusses the interview approach for the validation and shows the results, while Section 2.4 presents the survey and its results. The chapter is finally concluded in Section 2.5.

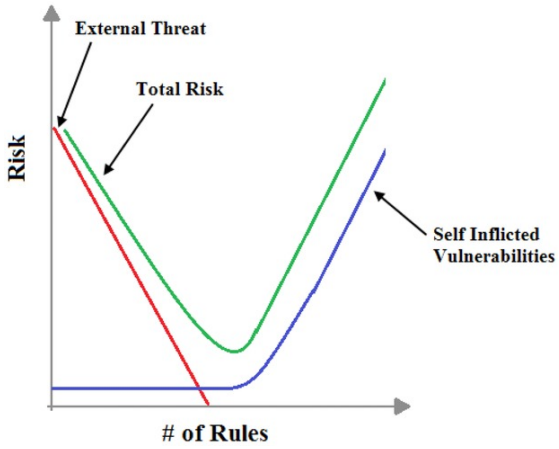
2.1 ELEMENTS OF INNOVATION

2.1.1 Related Fields of Study

To assess risks, the context in which we assess the system needs to be defined (Refsdal et al., 2015). The establishment of the context is important, but an often neglected step in the risk assessment process (Cherdantseva et al., 2016). Before identifying risks, the context determines where and how we identify potential threats. We establish the environment of the system to enable the identification of external threats, whereas the goals, objectives, policies, and capabilities concerning the system to determine the internal context (Refsdal et al., 2015). In this study, the establishment of the context results in elements specific to innovation projects. These elements are determined based on the unique aspects of innovation projects, as found in literature and practice. Other fields, such as Supervisory Control And Data Acquisition (SCADA) systems, IoT, and smart cities, have these elements more clearly defined. Radanliev et al. (2018) identify the most prominent IoT risk vectors in their literature review. They find cloud technologies, real-time data, autonomous machine decision, and communication risks as the risk vectors most significant when assessing cyber risks of IoT. For SCADA systems, the human factor within a system is found as a prominent component. Cherdantseva et al. (2016) found, besides the human factor, expert opinion involvement and overcoming attack- or failure orientation as important components. Smart cities, as a concept, are closely linked to innovation. Technical innovation meshes with the cities' innovation in the policy and management aspects (Nam and Pardo, 2011). The innovation of smart cities creates new threats and dependencies. Vitunskaite et al. (2019) find collaboration and open innovation as fundamental components to the success of smart cities. Mitigation measures should counter new threats and dependencies to avoid them from occurring. Despite the awareness of cybersecurity concerns, Vitunskaite et al. (2019) argue that many smart cities still fail to identify and mitigate these risks appropriately. Their study proposes the lack of appropriate standards and guidance, clearly defined roles and responsibilities, and a common understanding of key security requirements to be the main causes of this deficiency. Their suggested framework focuses on the three concepts of technical standards, cybersecurity measures, and an effective third party management approach (Vitunskaite et al., 2019). The literature review results in four elements of innovation projects. Note that there is a difference between the elements of innovation and the cyber components this chapter aims to uncover. The link here is that certain innovation elements identify the cyber components. Next, we introduce the elements of innovation.

2.1.2 Freedom for Innovation

To define elements of innovation, we first explicitly define innovations as a concept. More specifically, the characteristics of innovation projects should be made clear. Mihić et al. (2018) identify the characteristics of energy innovation projects. First and foremost are the innovative features of these innovation projects. Innovations tend to have processes and an approach that is explorative and experimental, accompanied with high risks and failure rate. According to the framework proposed by Bowers and Khorakian (2014), risk management should be involved in each development phase of the innovation, while concurrently risk management must be deployed selectively. Excessive use of risk management in innovation could stifle creativity, a critical component to innovation (Bowers and Khorakian, 2014). Stifling creativity and therefore limiting the development of innovation is not desired. We observe a trade-off between enabling creativity and limiting risks. Risk management literature covers this trade-off, without the explicit definition as a trade-off. Restricting the set of rules and regulations in risk management stimulates innovation. A select number of rules limits the risk increase of cybersecurity in innovation (Gisladottir et al., 2017). Figure 2.1 shows the relation of both internal and external threats with the number of regulations. The graph visualizes the trade-off between innovation and rules. Where rules are needed to reduce the risk from external threats, the amount should not enable internal vulnerabilities to rise at the same time. In this study, we conceptualize this as the freedom for innovation element. Besides the creativity factor, this also includes the tolerance of failure. Tolerance of failure is a concept in innovation which affects the level of risk that innovators are willing to take. Hutchison-Krupat and Chao (2014) found that higher tolerance for failure increases an individual's willingness to take risks in the innovation strategy. Firms with a higher tolerance for failure tend to be more lenient towards innovating and having more uncertainty in their research and development (Custódio et al., 2017). This leniency benefits the freedom to innovate for projects, while more risk is accepted, and firms must assess the risks accordingly.



"The red line represents the risk from external threats; the blue line represents the risk from internal vulnerabilities; and the green line represents the combined risk from external threats and internal vulnerabilities". Reprinted from *Resilience of Cyber Systems with Over- and Underregulation*, Gisladottir et al. (2017, p.1645)

Figure 2.1: System risk is a function of the number of rules

2.1.3 Roles and Responsibilities

Other fields of study name the human factor as an important element. Literature defines this element in various ways. Ganin et al. (2017) define this human factor as the social domain. In their framework, human factors relate to personnel-related vulnerabilities. The personnel' background, their awareness & training, access control, and loyalty & well-being are criteria to determine the risk of the social domain. Personnel is also influencing the innovativeness of organizations, where especially the top of organizations, can spur innovation. Custódio et al. (2017) suggest that the chief executive officers of firms who acquire knowledge beyond the

firm's technological domain and with a tolerance for failure spur innovation within their organization. In addition to the domain of projects' personnel, the human factor also involves other, sometimes external stakeholders. Mihić et al. (2018) find innovation project teams generally to be multi-disciplinary and to consist of many stakeholders with often conflicting interests and goals, resulting in a difficult decision-making process and consequently plentiful of (new) threats from the environment of the system. This study conceptualizes the human factor in the element of roles and responsibility. This element incorporates both internal and external stakeholders of the innovation project and the communication between them. The relation between stakeholders and the responsibilities they hold are indications of their influence on the innovation process. The roles and responsibilities are similar to the human factor in information security. The added dimension of humans being the target of a (cyber) attack or unknowingly participating in one is unique to cybersecurity (Von Solms and Van Niekerk, 2013).

2.1.4 Information Architecture

A key element for innovation projects is the explorative or experimental processes of the system (Mihić et al., 2018). Often does this involve information from software components that are prone to cyber threats. Operational trade-offs are one of the main reasons that cyber-attacks are still occurring and are successful, despite cybersecurity efforts (Hughes and Cybenko, 2013). The information security and cybersecurity standards and guideline set these operational trade-offs which are to safeguard the confidentiality, integrity, and availability (CIA) of information (Refsdal et al., 2015). Information should be protected from unauthorized access (Confidentiality), unauthorized modifications (Integrity), and have the ability for end-users to derive a certain benefit from the system (Availability) (Hughes and Cybenko, 2013). Information in itself is categorizable in the different forms or systems of how information is derived. Radanliev et al. (2018) identify risk vectors for the Internet of Things systems. The Information Architecture element proposed in this study categorizes three out of the four recognized vectors, namely cloud technologies, real-time data, and autonomous decisions. These risk vectors involve some software or information architecture that we consider when assessing the cyber risks to the system. We test each of these vectors against the trade-offs for confidentiality, integrity, and availability.

2.1.5 Physical Security

The physical elements are viewed as critical in the security of a system (Pearson, 2011). The access to machines, network attach points, and other hardware are prone to physical attacks to the system. Pearson (2011) argues that the physical security of the system is, at times, impossible to guarantee due to the location of the physical components. The author uses smart meters in customers' homes for the smart grid as an example. The internal networks of a system are prone to attacks, even without connection to external networks such as the internet. Innovation projects often involve a cyber-physical system. This type of system contains physical components with the ability to gather data from the physical world and process this within the network of the system (Peng et al., 2013). Data gathering from these components, such as sensors and actuators, can be used in cyberattacks without the need for attackers to intrude the system's cyberspace.

2.2 CYBER COMPONENTS OF INNOVATION

2.2.1 Prior Work

We first review literature that aims at identifying key components, elements, and vectors for cyber-physical systems. Radanliev et al. (2019) identified risk vectors of IoT systems from a literature review. IoT risk vectors were grouped together or not considered, as they concluded that analyzing every single vector was out of their study's scope (Radanliev et al., 2019). Focusing on the prominent vectors benefits the study by presenting general vectors that apply

to a broad range of systems. However, these general vectors provide limited details on the system and its processes. Veeramany et al. (2019) make use of more specific elements to form their framework for risk-informed autonomous adaptive controllers. Elements are categorized based on their function in the system. The use of a framework provides a structured presentation of the system while maintaining a higher level of detail in the identification of elements. This study aims to present cyber components of innovation projects. Innovation projects indicate a wide variety of projects to our scope, which asks for a generalizable list of components. However, to assess the risks of a system later in the study, we need to establish a level of detail for the components which enables us to assess the risk threats to a project's system.

2.2.2 Identifying Cyber Components

The elements specific to innovation projects in the previous section establish the framework in which we can conceptualize innovation projects. The elements form the core of innovation projects, consisting of various components. This study uses the term 'component' where other studies also used terms such as 'elements' or 'vectors'. Literature provides no specific reason on which term to use. We derived the term component from standards and guidelines such as ISO and NIST and terminology used by Refsdal et al. (2015).

When assessing the cyber components of innovation projects, not all elements are involved. The freedom for innovation element, for instance, does not contain cyber components. Cyber components might influence the freedom for innovation, but the element itself does not consist of such components. Figure 2.2 shows the elements of innovation projects and where we find cyber components. For the most part, cyber components are part of the Information Architecture element. This element contains components that are prone to cyber-attacks and crucial to technological development. However, most innovative projects are a cyber-physical system, meaning that these projects work with a system that combines the components from the Information Architecture element with those of the Physical Security element. The physical security of the system contains components that are communicating with software components, and are prone to physical attacks at the same time. For that reason, the cyber components do not solely fall under the Information Architecture element in Figure 2.2, but also are (partly) covered by the Physical Security element.

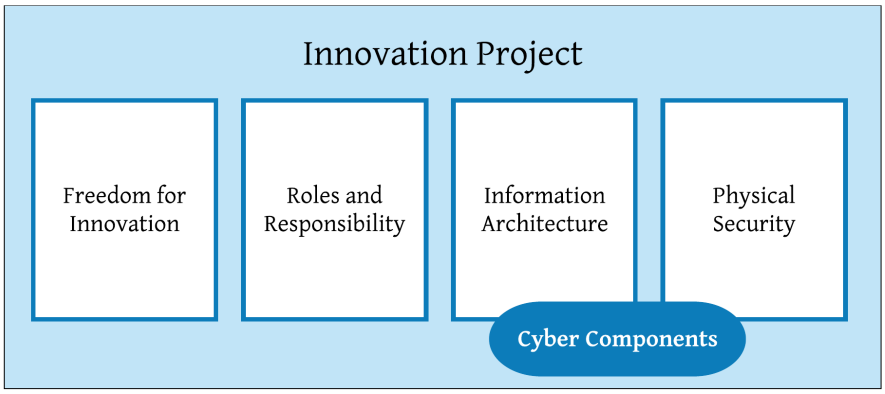


Figure 2.2: Cyber components within the 'elements of innovation projects' framework

2.2.3 Cyber Components from Literature

We use a literature review to compile a list with cyber components for innovation projects. Both a structured search and an explorative snowball search are used as methods to come up with suitable literature. Jalali and Wohlin (2012) concluded that one of both methods did not outperform the other. This study uses both methods to cover as much scientific ground as efficiently possible. The literature review process is visualized in Figure 2.3. For the search query in Scopus, we set two requirements for the eventual results. First, we need a type of assessment or analysis of risks. This need leads us to the following search term:

Table 2.1: Categories of cyber components

Category	Description
Data collection	Components that collect data in the physical world
Communication	Components which enable communication between parts in a system or between separate systems
Data processing	Components that either store collected data or perform some type of action based on data collecting components
Control	Components that control the physical components of a system and monitor performances
Physical	Components that are placed in or are part of the physical world

`(\risk assessment" OR \risk analysis")`. Secondly, we seek components of systems in related fields of study. As discussed in Section 2.2.2, different terminology is used in literature. The literature review of this chapter found components, elements, and (attack) vectors most commonly. Therefore, we include these three terms in the search. This results in the following search term: `("cyber components"OR"cyber elements"OR"attack vectors")`. We use the above two search terms combined with the command `AND` to find results that include both requirements for the results. The second term in between brackets is used to find the cyber components.

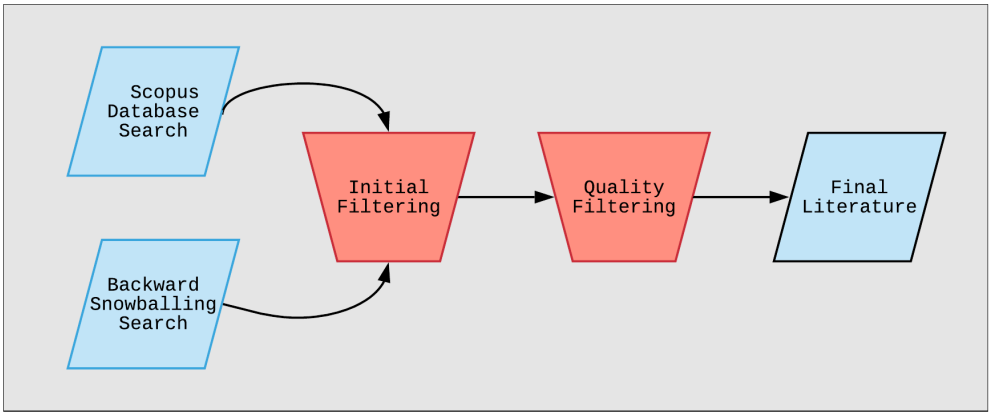


Figure 2.3: Literature review process for the cyber component list

The Scopus search resulted in 63 articles. Of these 63, only two aren't written in English, leaving us with 61 results. We set specific quality measures for the further filtering of the search results. We search for cyber components of systems in related fields of study to innovation. Studies in other scientific areas, such as health care, military, and supply chain, are not considered here. This filter led to a list of ten remaining results, which we assess in greater detail. The last filtering focuses on finding potential cyber components mentioned in the articles. Common ground for excluding literature in this phase is another use for the term component. From the snowball exploration of the literature review, we find seven articles matching the quality criteria set for the results from the Scopus search. Survey reviews, such as Cherdantseva et al. (2016) and Giraldo et al. (2017), are used as starting points to find cases in related fields of study mentioning components of systems. Table 2.2 shows the literature used to compile the cyber component list. The table presents the subject of the study, the publishing journal, and the search method for each article. The compiled list of cyber components shows the source in the last column (see Table 2.3). The letters correspond to a source, as listed in Table 2.2. For example, the component' smart meters' is found in sources c and h. According to Table 2.2, that refers to the risk assessment of cyber-physical systems of Ashibani and Mahmoud (2017) and to the risk assessment of smart power grids of Sun et al. (2018). Section 2.2.4 addresses the components and their sources in greater detail.

Table 2.2: Literature review cyber components

	Source	Subject	Journal	Search method
a	Torkura et al. (2015)	Cloud Platforms	Proceedings of the 10th International Conference for IT and Secured Transactions	Scopus
b	Saripalli and Walters (2010)		Proceedings of the 3rd IEEE International Conference on Cloud Computing	Scopus
c	Ashibani and Mahmoud (2017)	Cyber Physical Systems	Computers & Security	Snowball
d	Stergiopoulos et al. (2018)		Computer Networks	Scopus
e	Kettani and Wainwright (2019)	Cyber Systems	Proceedings of the 2nd IEEE International Conference on ICT	Scopus
f	Stouffer et al. (2011)	Industrial Control Systems	National Institute of Standards and Technology Special Publication	Snowball
g	Radanliev et al. (2019)	Internet of Things	Cornell University	Snowball
h	Sun et al. (2018)	Smart Grid	International Journal of Electrical Power & Energy Systems	Snowball
i	Liu et al. (2012)		IEEE Communications Survey & Tutorials	Snowball
j	Komninos et al. (2014)		IEEE Communications Surveys & Tutorials	Snowball
k	Ghena et al. (2014)	Traffic Infrastructure System	Proceedings of the 8th Workshop on Offensive Technologies (USENIX)	Snowball

2.2.4 Cyber Components List

We grouped the cyber components into five categories (see Table 2.3). We formed the categories by assessing the literature and the categorization used in other reviews and surveys. Some components classify for multiple groups. In this case, we categorize these components at our discretion. Expert interviews later on in the study will validate these choices (see Section 2.3). Each category has an 'other' component, which keeps the category open for additions of a specific case. This subsection continues with the explanation of the cyber component per category.

Data collection - Radanliev et al. (2019) discuss cyber risk vectors of IoT systems. Among the data processing components, discussed later on, we categorize one vector as data collecting, namely real-time data. Radanliev et al. (2019) pointed out the trade-off between the necessity of real-time data for IoT and the increase in risks due to the use of real-time data. Various studies mention real-time data when assessing risks, although not always as a component. We find other data collecting components in cyber-physical systems, where sensors serve a prominent role. The perception layer, where sensors are used to collect information for the system, is also known as the sensor layer (Mahmoud et al., 2015). Ashibani and Mahmoud (2017) distinguishes various types of sensors, such as smart meters and cameras. The list in this study defines 'other type of sensors' specifically, besides the standard 'other' component for each category. This option is to limit the number of the components listed, as there is a wide range of sensors. We list two types of sensors as components. Smart meters have a prominent role in the security of smart grids, as these meters are often placed in spaces with outsider's access and therefore have a high vulnerability (Sun et al., 2018). Cameras are the second sensor component. Ghena et al. (2014) discuss the new role of cameras, as cameras now also serve as an autonomous inspection and detection sensors.

Communication - The communication group contains components which enable communication between components and system. Various studies address the threats and vulnerabilities that come with communication in a system. However, Ashibani and Mahmoud (2017) specifically discusses the different types of communication components. They discuss the cyber-physical system in a three-layer model of perception, transmission, and application of data. Both wired and wireless networks are considered as transmission components, whereas the authors grouped communication through satellite in the perception layer. In the smart power grid, the use of GPS is used to have substations communicating with the control center (Sun et al., 2018). This study considers three types of communication methods, namely through landline (wired), through mobile line (wireless) and satellite (GPS). Sun et al. (2018) discuss

Table 2.3: List of Cyber Components

Category	Component	Source
Data collection	Real-time data	g
	Smart meters	c,h
	Cameras	c,k
	Other type of sensors	c
	Other	
Communication	Communication through landline, power grid line	c
	Communication through mobile line	c
	Communication through satellite	c,h
	Human Machine Interface	h
	Other	
Data processing	Data processing/analysis tools	d
	Cloud technologies	a,b,d,g
	Offline data storage	d,e
	User Interface	a,d,e,i
	Other	
Control	Servers	d,h
	Firewalls	h
	Anti-viruses	h
	Feeder protection relays	d,h
	Malfunction Management Units	h,k
	Autonomous decision-making	c,g
	Other actuators	c
	Other	
Physical	Accessible hardware (for insiders only)	d,f,j
	Accessible hardware (for outsiders)	f,i,j
	Network access points / Points of entry	b,c,f
	(Ecological) environment that can affect hardware	f
	Other	

another communication method between humans and machines, which is particularly prone to cyber-attacks. Operators use human machine interface (HMI)s to assess the operation of machines in the system.

Data processing - Continuing from the data collecting category, data processing components either store collected data or perform an action based on information from data collecting components. This category also includes components that can both collect and process data (or initialize the processing step), such as actuators (Ashibani and Mahmoud, 2017). Among actuators, there are autonomous decision-making actuators. In IoT systems, autonomous cognition is required, but the autonomous machine decisions do bear more cyber risks to the system (Radanliev et al., 2019). Similarly to sensors, we distinguish multiple types of actuators. The component 'other actuators' leaves room for innovators to determine what their actuators are. Actuators and sensors can feed information to other parts of the system. The communication from data collecting to data processing and data storage are particularly prone to cyber attacks (Kettani and Wainwright, 2019). Stergiopoulos et al. (2018) discusses these processing components as assets of cyber-physical systems. In their study, user interface and data analysis software are closely related to data storage, both offline and in the cloud. These components are constantly communicating with each other, and disruption in that process could have great consequences. Offline data storage is in the development of technology replaced by cloud technology. The cloud has the advantage of being able to store and process data and make autonomous decisions. With this new technology, new threats and vulnerabilities emerge. Torkura et al. (2015) exemplify this with vulnerability scanners, which now must address security issues between a host and the guest operating system. Clouds often operate in open software to ensure accessibility to a wide variety of clients. The liability of the cloud operating system and the security of information rank among the top concerns of small and medium businesses for using cloud technology (Saripalli and Walters, 2010). The 'User Inter-

faces' component includes operating systems. With cloud technology, we find that different component within a system can run on different operating systems. Liu et al. (2012) also include customer interfaces when considering operating systems. Customer interfaces are accessible from the customers' side of the system, resulting in security issues for the system that is depending on the threat awareness of customers. Software and hardware updates should tighten the security and information from the customers should be validated to prevent the use of manipulated information (Liu et al., 2012).

Control - The fourth group consists of components which serve a controlling role in the system. The operations of the system as a whole and individual components are monitorable. This group closely connects to the communication group. We can see a component as HMI as a controlling component. However, with HMI components, the machine is communicating with human entities, who are in control of the operation. Sun et al. (2018) cover many controlling components in their assessment of cybersecurity of power grids, where different controlling commands are in place to keep the operating system running. The servers in the power grid's ICT system are used to control the transmission and distribution over the grid. Sun et al. (2018) point out that security policies use firewalls for the threat mitigation of control systems, despite their limitations. These security policies can involve multiple components, amongst them, are anti-viruses, feeder protection relays, and malfunction management unit (MMU)s. Feeder protection relays have several capabilities. As control components, relays can support communication protocols and serve as a filter to communication noise on the system's router (Stergiopoulos et al., 2018). MMU serves as a controlling component in smart traffic infrastructure systems (Ghena et al., 2014). MMUs are built-in safety mechanisms that can override controllers in the system if an error occurs.

Physical - As seen in Figure 2.2, the cyber components are also partly covered by the physical security element of innovation. Therefore, we include several physical components, as well. Hardware placed in the real world is center in this category. We discuss several hardware components in the previous categories; the components in this category involve the security of these hardware components. Stouffer et al. (2011) discuss the physical and environmental protection of the system with the protection of physical locations and access control to the system. The protection of physical locations is divided into internal (for insiders only) and external (both insiders and outsiders) accessibility. Liu et al. (2012) found the external accessibility in the smart grid systems, where customers interface with off-site placed smart meters, prone to outsider attacks. Accessible hardware on-site gives organizations more control in security, for instance by having security surveillance on the organization's perimeter, establish zones with physical protective boundaries, and have control over the essential services of the organization (Stergiopoulos et al., 2018). Network access points, or points of entry to the system, is a component that needs protection from (cyber) threats. Access monitoring systems, such as surveillance cameras and sensors, and access limiting systems, such as security devices and identification systems, are measures for the protection of points of entry (Stouffer et al., 2011). The authors specify heavier protection for cases with large installations, where tracking devices are used to track every movement within the facility of entities such as employees and vehicles. Most network accesses in cyber-physical systems involve the communication line through either radio channels or wireless networks (Ashibani and Mahmoud, 2017). Access control and network encryption are security measures for the cyberspace, but the physical access (e.g. radio towers, base router stations) need security measures as well. The final physical component considered in the list is '(Ecological) environment that can affect hardware'. The need for this component comes from the distinction between attacks and intrusions and malfunctions. The accessible hardware components cover attacks and intrusions. Stouffer et al. (2011) define environmental factors such as the temperature, humidity levels, and stability of the site ground. Heating, ventilation, and air conditioning (HVAC) are an environmental control system to ensure the necessary temperature and humidity conditions during operation and in emergencies (Stouffer et al., 2011). The authors discuss the increasing security roles of HVAC and fire systems due to the connection of process controls and security systems, and the cyber access to those components (Stouffer et al., 2011).

2.3 EXPERT VALIDATION

2.3.1 Interview Approach

We derived cyber components from literature, mostly concerning related fields of study, such as IoT and smart technology. The data collection specific to innovation projects from literature was limited. Expert validation can increase the validity of the found components for innovation projects. A semi-structured interview was used to gain in-depth knowledge from experts in the field of cybersecurity and innovation. The interviews are conducted in a semi-structured manner to provide the interviewees with the freedom to share their knowledge on cybersecurity of innovation, while still structuring the interview around the proposed cyber components. Appendix A presents the full breakdown of the interview proposal. Table 2.4 shows the interviews used for expert validation. We analyze the results from these interviews according to a deductive approach. The deductive approach starts with a theme or theory determined before the analysis (Zhang and Wildemuth, 2009). In this case, the list of cyber components is the starting point of the analysis. We gather the acquired data from the interviews to validate this list.

Table 2.4: Expert validation interviews

#	Interviewee	Organization	Status
1	Professor Safety Science	TU Delft	Responded via e-mail on August 12, 2019
2	Project Manager	BRIGAID	Meeting in person on July 30, 2019
3	Information Security Officer	ABN Amro	Conducted in person on July 29, 2019

2.3.2 Results

Three interviewees were chosen based on their occupation and field of work. Since innovation is a broad concept, we acquire knowledge from both the academic and business field. The last interviewee is the project manager of BRIGAID, who is more knowledgeable about the projects specifically addressed in the BRIGAID program. Coincidentally, the three interviews are each conducted in a different form. The Professor in the Safety and Security Science group at the Delft University of Technology responded by e-mail, we quoted BRIGAIDs project manager from an open meeting and interviewed the IT expert (named Information Security Officer) at ABN Amro in person. The semi-structured interview created a freedom to discuss innovations and cybersecurity in greater detail, this to generate information for other purposes in this study as well. We used a word table as a coding technique to structure the qualitative data from the interviews. Appendix A presents the word table (Table A.1) in its entirety. We derive the results from the themes in the word table. These themes are created from the raw data of the interviews. This subsection describes the results we use to validate the cyber component list that we compile this chapter.

The cyber component list is a collection of components, elements, vectors, and assets which literature defines. Different sources come up with differing components, and there is a subjective feel to the selection of some of these components. Components are categorizable in different manners. We conclude that the categorization should not be leading when interpreting the results later on in this study. We find that the perspective used to assess a system plays an important role. Different perspectives are defined, which we present as secondary level themes of the primary cybersecurity theme in Table A.1. The current cyber component list follows from a rather physical perspective, where the focus is on physical components, rather than the data that the system or the communication lines that transmit the data use. A technical perspective would also look at an individual component but then focus on the links to the system and other components. A contrasting perspective to the physical perspective is the process one. The process perspective focuses on the main communication line and expands from there to explain the system and its components (Information Security Officer, ABN Amro, 2019). The different perspectives identify different components of the system, even though we assess the same system. Prioritization of the components comes in play here.

For example, we define different types of communication components, such as communication over a landline, mobile line, and GPS. This distinction is made to distinguish the different types of communication means. In other perspectives, such as the technical or data flow perspective, the different means play no significant role. When assessing communication through a technical perspective, components like communicating servers come to mind, or we address the internet gateway in between the servers. The validation raises the importance of certain components, whereas the importance of other components decreases. Another feature of the components is the ability to switch them from categories, or account them over more than a single category. For example, the actuators in the control category were switched from the data processing category based on the interview results. Actuators were initially seen as data processing component which have the ability to make decisions. This feature is a greater fit with the control category. Think, for instance, of a moveable water gate which adjusts is height based on the water level (Professor Safety Science, TU Delft, 2019). We conclude that there is not a single view for assessing systems; the used perspective determines what components we consider in our assessment. We also conclude that the other elements of innovations, as we define in Section 2.1, play significant roles in the cybersecurity assessment, and the components on the list cover only partly the system we seek to assess.

2.4 INNOVATOR SURVEY

This section discusses the identification of key cyber components through the survey sent out to the BRIGAID innovators. We use a survey for two purposes. First, to gain information on the structure of the projects in terms of cyber components. Second, to acquire insight into what the key cyber components are when assessing the cybersecurity of innovation projects. We discuss the survey design and report the results, after which the key cyber componets are presented. For the survey design as sent out to the innovators, see Appendix C. For the survey design, we loosely follow the steps from Pfleeger and Kitchenham (2001). Due to the rather small scale of this survey, we merge some steps in the process into one step.

2.4.1 Survey Objectives

The first step is setting objectives that are both specific and measurable. The objectives for this survey come from the sub-question of this chapter, which is: *What innovation projects within the BRIGAID project can provide the broadest variety of cyber components?*. The survey should reflect this question by gaining both objective and subjective data on cyber components and innovation. The objectives of this survey are as followed:

1. Determine the key cyber components for cybersecurity of innovation projects
2. Determine the most valued cyber components for cybersecurity of innovation projects

Key cyber components in this study concern cyber components that we find most commonly in the innovation projects. A subjective valuation of the cyber components aims to meet the second objective.

2.4.2 Survey Planning and Schedule

The second step is to plan and schedule the survey. From the research flow diagram in this study (see Figure 1.3), the process of selecting the projects for the case study is preceded by the conceptualization of the cyber components (see Chapter 2. The scheduling of the survey depends on the preceding steps of the research flow. Within the planning, the survey is sent out on August 8, 2019. For a period of three weeks, innovators can respond by filling out the survey through the online platform SurveyGizmo (SurveyGizmo, 2005). The response period is limited but necessary for the remainder of the study to be carried out according to the schedule. SurveyGizmo provides a free-of-charge platform to host surveys. The limit to responses per month supersedes the number of innovation projects within BRIGAID. Elbeck (2014) reviewed the host options for surveys that are free-of-charge. SurveyGizmo ranked top

five in popularity and satisfies the needs for this study, such as data export to CSV format, online visibility, and the ability for respondents to fill in the survey through e-mail and an online link (Elbeck, 2014).

2.4.3 Questionnaire Design

The fourth step in the process is the design of the questionnaire (see Figure 2.4). For efficient data acquisition, we conduct an unsupervised survey, i.e. innovators can respond to the survey by e-mail or via a weblink, without the supervision of an interviewer (or questioner). We present an introduction to the survey at the beginning to provide the respondent with information. The introduction addresses the goal of the survey and provides some theoretical context. The theoretical context is important, as it provides the respondents with the definition of cyber components in this research's context. Finally, we address the privacy and data use, before expressing our gratitude for the time and effort.

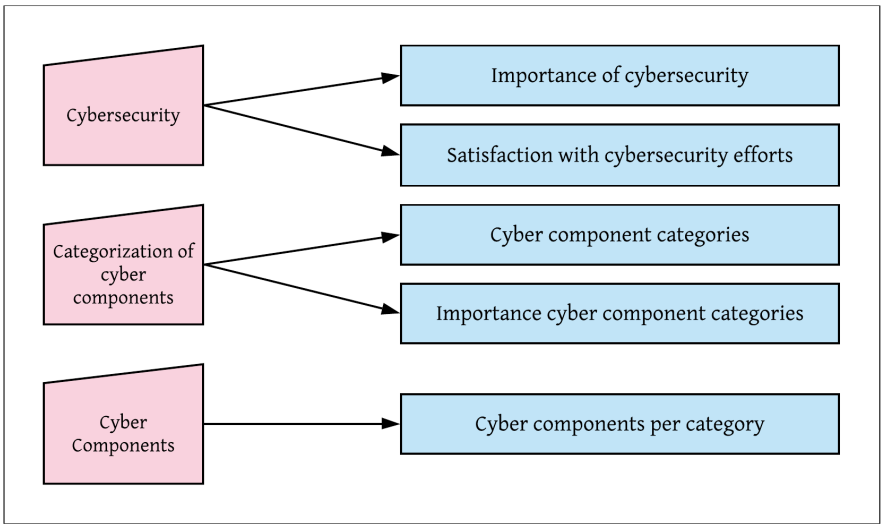


Figure 2.4: Modeling process of the survey

After the introduction, the first questioned ask participants to choose their project from a dropdown menu. The projects of BRIGAID are known, so a dropdown menu is used to ensure the use of the project name as known from the BRIGAID portfolio. The next questions on the cybersecurity efforts of the innovation projects. We ask the respondents to rate the importance of cybersecurity to their project and how satisfied they are with current cybersecurity efforts. A 6-point Likert scale answers the rating questions. Nemoto and Beglar (2014) discuss the Likert scale as a measurement for the psychological construct of a person's cognition. The scale moves from the weakest endorsement of the item to the strongest (see Figure 2.5).

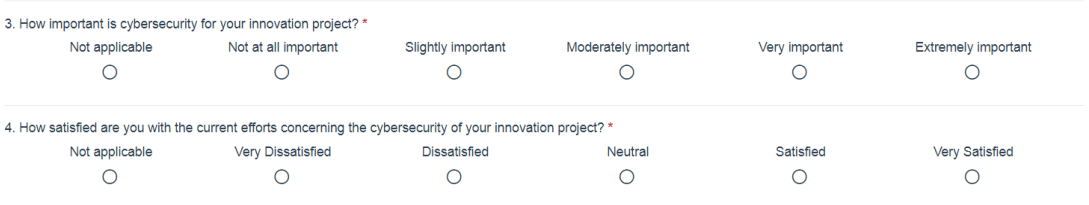


Figure 2.5: Capture of the survey questions on the perception of cybersecurity

The next page of the survey involves cyber component categories. We provide the respondents with a brief introduction and description of these categories. In an open-ended question, the respondents are asked their opinion on the chosen categorization of the components. Open questions have the benefit of not constraining respondents to answer options (Schonlau and Couper, 2016). The downfall is that these questions are more challenging to analyze, due to

the wide variety of answering options. The limited pool of respondents in this study makes the analysis of the results possible.

The third and last page of the survey contains the actual questionnaire on the specific components, as compiled in Section 2.2 (see Table 2.3). For each category, we give the list of components with checkbox answering options. Respondents provide additional components through an open 'others' option. When they check the 'other' box, the respondent is required to fill the box in with an answer. This requirement ensures that the option 'other' is accompanied by a component. After selecting the components that are part of the project's system, the respondents are asked to rank the categories from most important to least important. The answer box is for open answers, so the respondents have freedom in how to express their ranking of the categories. Finally, an open answer box provides space for remarks or recommendations, and the respondents get the option to leave any contact information if they are willing to discuss the cybersecurity of their innovation project in greater detail.

2.4.4 Results

The pool of respondents consists of the innovation projects which affiliate with the BRIGAID program by having their information on the Climate Innovation Window. The finite pool consists of 121 innovation projects. Of those 121 projects, we received a completed survey response from 18 projects, resulting in a response rate of nearly fifteen percent.

We have measured the composition of the innovation projects' systems according to the compiled list of cyber components. Respondents were asked to select the components which are present in their system. We gave the respondents the freedom to add categories and components which they deem important in their system. We discuss the process of adding these components in Appendix C and present the results in Table C.3. We present the results of the most occurring components. We also asked the innovators about their perception of the importance and satisfaction they feel when assessing the cybersecurity in their project. A breakdown of the complete survey results is presented in Appendix C.

The most occurring components are presented in Table 2.5. While we conclude from the expert interviews that the categories are not of the main importance, we present the number of occurring components per category (see Figure 2.6). The most occurring component is the *'data processing/analysis tool'*. Most projects use some type of data processing tool. The survey did not ask in detail what such a tool entails. The second component in terms of occurrence is *'Human-Machine Interface'*. This communication component occurs in the same number of projects as *'Servers'* and *'Accessible hardware (for insiders)'*. To identify key cyber components, we assess the most occurring components of projects of innovators who perceive the importance of cybersecurity either as moderately high or extremely high (see Table 2.6). This filter presents components which occur in systems where the cybersecurity of that system is highly rated. We do the same for projects with (very) satisfied innovators concerning the current cybersecurity efforts (Table 2.7).

Figure 2.7 presents the identified key cyber components. The list composes the most occurring components from the survey with some additions. The first addition is the communication line component. The survey showed communication through the mobile line as a frequently occurring component. When considering innovation projects solely with high satisfaction with current cybersecurity efforts, communication through landline is a frequently occurring component as well. The interview with the Information Security Officer showed that the mean of communication is not of importance in his view. The fact that components communicate is the main takeaway. Therefore, we include the communication line as a collective component for all three communication methods (mobile line, landline, and satellite). We also find sensors to be a collective component, with *'smart meters'* as an often occurring component. The cyber component list includes sensors, and we gave respondents the option to add sensors from their project's system. The results show that drones were a missing and unique sensing component not included in the initial list. We include *'sensors'* as key cyber components.

Table 2.5: Ten most occurring components

Component	Count
Data processing/analysis tool	13
Servers	12
Anti-virus	11
Accessible hardware (for insiders)	11
Human Machine Interface	10
User interface	9
Firewall	9
Communication through mobile line	8
Offline storage	8
Smart meters	7

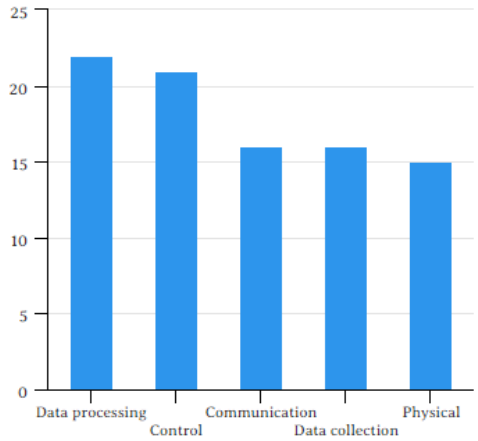


Figure 2.6: Number of components per category

Table 2.6: Components with high CS importance
Ten most occurring components in projects with high perceived importance of cybersecurity

Component	Count
Servers	7
Communication through mobile line	7
Offline storage	7
Data processing/analysis tool	6
User interface	6
Anti-virus	5
Firewall	5
Human Machine Interface	4
Real-time data	4
Accessible hardware (for outsiders)	4

Table 2.7: Components with high satisfaction
Ten most occurring components in projects with high satisfaction with cybersecurity efforts

Component	Count
Servers	7
Communication through mobile line	6
Offline storage	5
Data processing/analysis tool	5
User interface	5
Anti-virus	4
Firewall	4
Human Machine Interface	4
Real-time data	4
Communication through landline	4

2.4.5 Validity of the Survey

The previous subsection presents the results of the survey. The response to the survey was low, as only fifteen percent of the innovation projects responded to the survey. This subsection aims to consider the validity of our results. We also question what the validity means for the rest of the study's conclusions.

The low response to the survey poses numerous threats to the validity of the results. The external validity is of main concern here, as we aim to make generalizable claims based on the (survey) results. However, we also address other types of validity.

The external validity concerns validity threats that can reduce the generalizability of the survey results. The external validity is of special concern in this study, because of the general conclusions we aim to make for innovation projects based on the results of this study. One of the experimental effects the results of a survey can display is the novelty effect. With this effect, respondents show different behavior or answer questions different because they are taking part in a survey. This behavior shows in the satisfaction of the cybersecurity effort question. The results are skewed in solely positive responses, as no one responded with a dissatisfaction of the project's cybersecurity efforts. This positive result could be truthful, but the results would base better conclusions when, for example, an additional question was how much working hours or resources innovators allocate to the cybersecurity efforts of a project. These questions would result in numerical values, which we could compare to the size of the

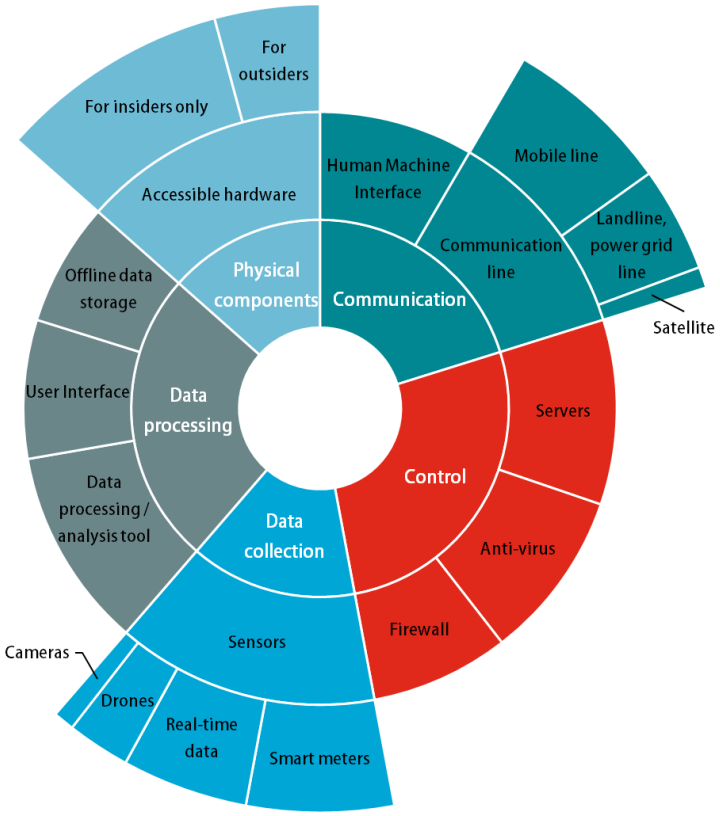


Figure 2.7: The identified key cyber components for innovation projects

project and the satisfaction of the innovator. This limitation is input for future surveys on this subject. In this study, we do not value the satisfaction score when choosing the cases.

The construct validity concerns the extent to which the survey measures the underlying theoretical construct it aimed to measure beforehand (Andrews, 1984). From the survey results, we can observe the occurrence of cyber components. The goal was to define key cyber components based on the survey results. Solely identifying key cyber components based on the occurrences of the components would not be representing the most important components. We could also involve the perceived importance of the cyber component categories to determine key cyber components. However, in the expert validation of the cyber component list, we concluded that the categories are modifiable and components can be assigned to different categories when assessing them from other perspectives. The expert validation also gave another option to address this issue, for instance by asking additional questions on the usage of components, such as a scoring system for the components regarding the extent of use (Professor Safety Science, TU Delft, 2019). The amount of transmitted data or the frequency in which the system transmits data are also legitimate questions. This limitation is input for future research on the topic and future surveys. In this study, we aim to address the issue with key cyber components by involving the risk assessments of Chapter 5. By observing what components are most involved in the high-risk threats, we can identify key cyber components.

In conclusion, the survey raises numerous validity concerns. We addressed the concerns and translated them to the conclusions we draw from them. The survey's main purpose was to identify representative cases for risk assessments. We chose for the survey, instead of a random selection, to make an informed choice. Therefore, the implications of this survey and its validity do not weigh heavily on the results of this study.

2.5 CHAPTER CONCLUSION

This chapter aimed to answer the first sub-question of this research: *What type of cyber components can be distinguished when assessing risks in innovation projects?*. First, we discussed the elements of an innovation project. Elements found in related fields of study and literature on innovation were used to compile a framework with four elements that form an innovation project. The freedom of innovation was found to be important and unique to innovation. The freedom to work in a system and improve it is an important trade-off with the security of that system. The human factor and human interactions merge in the roles and responsibilities element. The cyber part of innovation is covered by the information architecture element, while the physical security element covers the physical side of the system.

Within those last two elements, we identified space for cyber components. Cyber components are parts of the cyber-physical system of innovation projects, and we categorize them in five elements, namely components of data collection, communication, data processing, and control, and physical components (see Table 2.3). Experts in the field of innovation projects, cybersecurity, and security and safety science validated the list of cyber components. We found the categorization to be subjective and not leading when assessing key cyber components. The data from the interviews also showed the different perspectives with which we assess the cybersecurity of systems. We determine that the perspective for this study follows from the used risk assessment methodology. Figure 2.7 presents the cyber components we assess as key to the risk assessment of innovation projects.

The next chapter will focus on the innovation projects within BRIGAIDs portfolio. We select representative projects for the case study based on the cyber components that the projects' systems possess and the role of cybersecurity within that system.

3 SELECTING BRIGAID INNOVATION PROJECTS

This chapter sheds light on the subjects of the case studies in this research. The assessed innovation projects come from the BRIGAID portfolio. Section 3.1 describes the general purpose and objectives of BRIGAID. The Test and Implementation Framework (TIF) tool that this study aims to extend with a cybersecurity section is discussed in Section 3.1.1. We present the approach and results of achieving the main objective of this chapter, which is to identify representative innovation projects as cases to this study, in Section 3.2. Section 3.3 concludes the chapter.

3.1 BRIGAID

Increasing efforts are made to put climate adaptation high on the political agenda. We find efforts concerning the stimulation and support of climate adaptation measures on all scales ranging from the local to the international stage. The EU and its member states shift moreover towards the use of climate research and innovative measures in the decision-making. Examples of innovative adaptation efforts from the EU are the LIFE program and Horizon2020. (van Loon-Steensma, 2018).

BRIdge the **GA**p for **I**nnovations in **D**isaster resilience (BRIGAID), the objective of the project is already in the name. BRIGAID is a four year project under the European Union (EU)'s Horizon2020 (H2020) programme, which is in place to stimulate innovation. Integral, ongoing support from the organization should benefit innovators who focus on climate adaption. Guidance development of these innovations through the entire development cycle should result in more innovative projects that are ready for commercial deployment (BRIGAID, 2016a). BRIGAID aides innovators by providing the TIF and other practical tools designed to increase social, technical, and market readiness of innovations (Sebastian et al., 2019a). The projects within the BRIGAID portfolio should benefit from the tools and assessments by increasing their Technical Readiness Level (TRL), which is a measurement of the maturity level of innovations, ranging from 1 (basic principles observed and reported) through 9 (system ready for full-scale deployment) Figure 3.1.

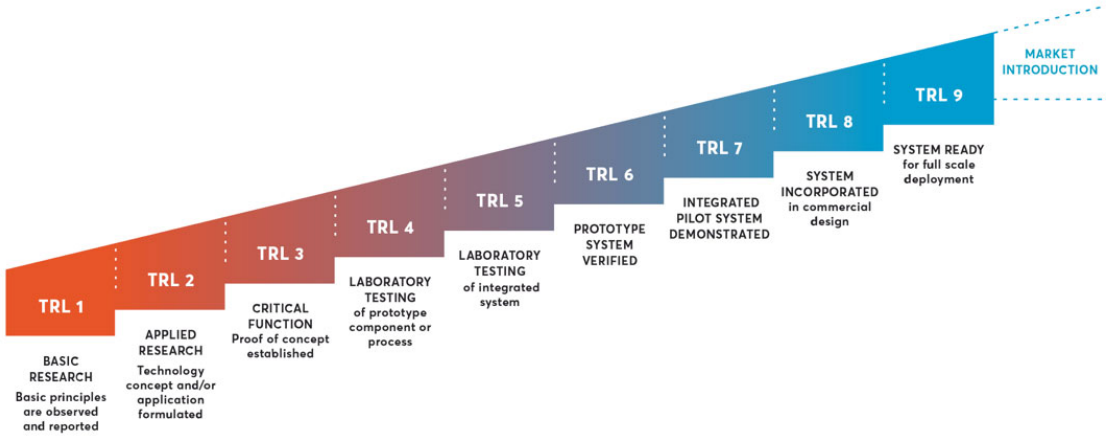


Figure 3.1: TRL Categories (BRIGAID, 2016b)

3.1.1 Test and Implementation Framework

The BRIGAID TIF is the main tool of the program. The tool should benefit climate adaption innovators by providing them with a self-assessment to raise concerns in their project from the development stage through the implementation of their project. The tool consists of 84 questions, divided over four categories. The answers translate to a score for the project to determine whether each categories' concerns are sufficiently covered. The tool is not a definitive assessment method, i.e. based on the assessment results concerns are being raised, not solved. The tool advises innovators to use it in three so-called stage-gates (Sebastian et al., 2019b). The first stage is before the validation in a laboratory setting. The second stage is before testing in an operational setting. Finally, the last stage of self-assessing the innovation project is before the deployment into the real world. The 'welcome' sheet of the tool covers these stages and discusses the use of the tool.

The tool divides the questions into five sheets, namely the general, technical, environmental, sectoral, and societal questions. Table 3.1 shows the structure of the questions in the tool per (sub)category. The last sheet of the tool contains a summary of the results. Innovators can use this sheet to assess the scores of their project per category through tables and graphs. The graphs are simple of nature and express the scores which the tables define in greater detail. This tabular form of communicating risk assessments was found to be more effective than graphical representation in IT systems (Labunets et al., 2017). The table distinguishes sub scores per category, which express the performance of a project on different aspects within a category.

Table 3.1: Questions per (sub)category in the TIF tool

Category	**Subcategory**	**Questions**
Technical		19
Environmental		21
	Design	*5*
	Impact	*10*
	Ecological impact	*6*
Sectoral		24
	Agriculture	*4*
	Energy	*4*
	Forestry	*3*
	Health	*4*
	Infrastructure	*6*
	Tourism	*3*
Societal		22
TOTAL		**84**

3.1.2 Innovation Projects

The BRIGAID portfolio is a collection of over a hundred projects all aimed at climate adaptation. The portfolio categorizes projects in the hazard the project aims to mitigate. Eight hazards specify the three generally used terms (floods, droughts, and extreme weather). Coastal and river floods divide the floods hazard. The difference, besides the location of the coast versus river, lays with the cause of the hazard. Coastal floods are generally caused by storm surges, whereas heavy precipitation or melted ice water causes river floods. Drought is a category that is not further subdivided and is, therefore, a hazard on its own. Extreme weather contains several hazards. The definition of heatwaves is a longer period of excessively hot weather. Wildfires often occur in regions facing droughts and heatwaves but is a hazard on its own. Uncontrollable fires in regions with combustible vegetation can result in critical situations. Storms are heavy rainfall, hail or other forms of precipitation combined with strong winds. This combination distinguishes storms from heavy precipitation, which is a hazard when causing (flash) floods exceeding drainage capacity. Lastly, there is the category of Multi-

Hazards, which can be assigned to projects when the innovation is overlapping categories. Table 3.2 gives an overview of the hazards. Different innovations are presented to address the same hazard.

Table 3.2: Hazards covered by the BRIGAID innovation projects

Floods	**Droughts**	**Extreme Weather**	**Multi Hazards**
Coastal Floods	Droughts	Heatwaves	Multi Hazards
River Floods		Wildfires	
		Storms	
		Heavy Precipitation	

BRIGAID also distinguishes the innovations by type of projects. Table 3.3 presents the topics for innovation projects in BRIGAID. The innovators select up to three topics to categorize their innovation projects. The topics represent an aspect of climate disaster resilience. Hazards around water can have different implications. Water poses a threat when water levels rise to a critical level, where floods may occur. The water safety topic covers this threat, with drinking water as another concern. The availability and quality of drinking water are topics for natural disaster resilience. Water availability may also concern the availability of irrigation water for agriculture. The last water topic in natural disaster resilience is rivers. van Loon-Steensma (2018) focuses on natural-based solutions, which are innovations that make use of the ecosystems. Agriculture and forests are other topics concerning the systems in nature. The energy sector closely links to climate change. Made efforts are renewable energy, sustainable energy use, and carbon footprint reduction. Despite the efforts in the energy sector, there are lots of challenges that complicate the energy transition, such as market failure and lack of resources (Owusu and Asumadu-Sarkodie, 2016). Natural disaster resilience isn't limited to nature. Urban areas are a topic where innovations in climate adaptation play a role as well. Oleson et al. (2015) address the concern of vulnerability and adaptive capacity of populations in the context of increasing heat stress days. The final topic links closest to this study. Disasters & ICT represents innovation projects that involve a type of ICT system. Innovations often include technological development, and cybersecurity plays a significant role in these projects.

Table 3.3: Topic categories within the BRIGAID portfolio

Topics		
Agriculture	Disasters & ICT	Energy
Forests	Nature-based Solutions	Rivers
Urban Areas	Water Availability	Water Quality
	Water Safety	

3.1.3 Climate Innovation Window

The establishment of the database of the innovation projects is focused on the Climate Innovation Window (CIW) as created by BRIGAID. The window is a web-based collection of all the innovation projects on climate disaster resilience which are in some way associated with the BRIGAID program. The website allows users to log in and communicate directly with innovators, while all the necessary information is available. Each innovation has a unique page where all available information on the project is provided, including public documents and a direct link to the innovator's website. This subsection presents the database and underlying data that is relevant for the study. The entire process of building the database from the web content is described in detail in Appendix B.

The CIWs webpage for each innovation has a fixed structure for the provided information. This structure simplifies data gathering through web scraping. Web scraping is a collection of methods and techniques that serve as automatic data gatherers. Web scrapers are particularly useful to structure data from the web into a database (Vargiu and Urru, 2013). We use the web scraping technique for web content mining. Web content mining differs from text min-

ing in the sense that text mining involves unstructured text, whereas web content provides (semi-)structured text (Bharanipriya and Prasad, 2011). For this study, we use the web scraper extension for Google Chrome by webscraper.io (WebScraper, 2019). The tool easily identifies the information categories and stores the data in a CSV-file. We clean the content and restructure it into a database in Excel. We use Python for the process of transforming the CSV-file into an Excel database. Figure 3.2 shows the process of the database design.

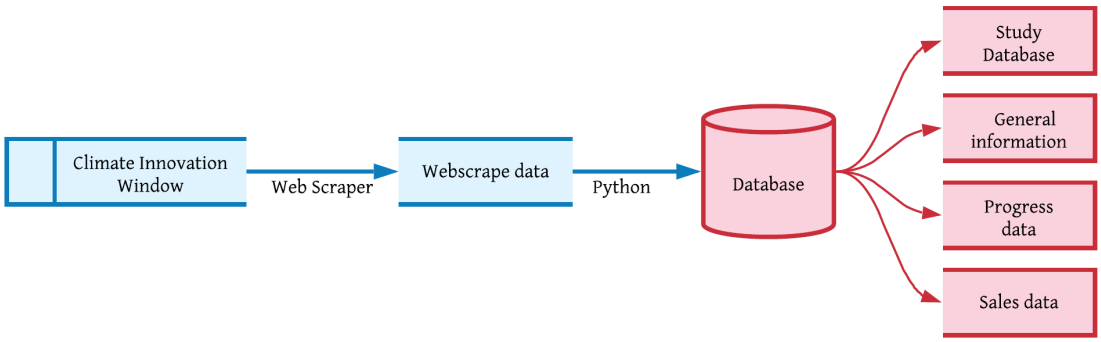


Figure 3.2: The process of the database creation

The database contains information for different purposes, such as progress sales data. In this study, we use the study database, which contains the necessary data for this analysis. Besides the name of the innovation project, we gather data from the file on the hazard and topic categories, and the Technical Readiness Level. This data provides an overview of which hazards and topics are mostly covered by the BRIGAID innovation projects, and what the average readiness level is of the innovation projects. Table 3.4 shows the descriptive statistics for the TRL values. The mean level is 5.56, meaning that the average innovation project in the BRIGAID portfolio is finished with the laboratory testing and is moving towards a verified prototype system (see Figure 3.1).

Table 3.4: Descriptive statistics for the TRL

Category	Mean	N	S.D.	Min.	Max.
TRL	5.56	121	1.663	2	9

The hazards and topics are categorical values, and therefore cannot be described by descriptive statistics, such as a mean or standard deviation. In our analysis of these categories, we test whether the categories are consistent with the expectations we have on their distributions. We assume that all categories are featured equally in the BRIGAID portfolio. We formulate the following hypotheses:

***Ho**: The data shows that the innovations are equally distributed among the categories*
***H1**: The data shows that the innovations are unequally distributed among the categories*

Note that the hazard and topic categories are tested separately on equal distribution, but the hypotheses are the same. We use the chi-square test for this analysis. The chi-square is fit for the analysis of categories and meets the condition of an expected value of the number of observations of at least five (Satorra and Bentler, 2001). Table 3.5 shows the results of the Chi-square test. The degrees of freedom (df) represents the number of categories minus one. The expected value is the expected number of observations for each category type if we assume an equal distribution among the observations. The Chi-square is the test statistic, following from the formula:

$$X^2 = \sum \frac{(O_i - E_i)^2}{E_i}$$

With O_i as the observed value, and E_i as the expected value. The p-value is the result of the test and represents the probability of the observed sample is as extreme as the test statistic

(Satorra and Bentler, 2001). We use a significance level of 0.05 and find that the Ho hypothesis of both the hazard and topic categories are rejected (since $p < 0.05$). Therefore, we conclude from the data that innovations are unequally distributed among the categories.

Table 3.5: Chi-square test results for the Hazard and Topic categories

Category	df	Exp. val.	Chi sq.	p
Hazards	6	17.000	60.235	0.000
Topics	8	19.778	55.494	0.000

3.2 SELECTION PROJECT CASES

This section discusses the process to the selection of the projects for the case study. We used a survey for two purposes. First, to gain information on the structure of the projects in terms of cyber components. Second, to acquire insight into what the cyber components are when assessing the cybersecurity of innovation projects. For the survey design as sent out to the innovators, see Appendix C. Section 3.2.1 describes the selection process, and the introduction of cases (Sections 3.2.2 and 3.2.3) serve as a brief insight into the projects' aims and structure of the systems involved. Chapter 5 analyzes the systems of the cases in greater detail.

3.2.1 Results from Innovator Survey

We use the most occurring components and perception of the importance of cybersecurity to identify two cases. The first case does not consider cybersecurity risks and is satisfied with current efforts. The second case has a high regard of importance for cybersecurity, with both cases containing a set of the identified key cyber components. We select projects containing at least the first four most occurring components (see Table 3.6). The hazard and topics of the projects are the last determining variable in the selection of cases. We seek two cases addressing different hazards to prevent specific conclusions for a particular hazard. The topic 'Disasters and ICT' should be covered by the project to ensure a case with a cyber system.

From the survey respondents, we find numerous potential cases. The first project is one of the cases with a satisfaction with current cybersecurity efforts. Of the six projects covering these requirements, only two cover the topic 'Disasters and ICT'. The two project addressed the same hazard of heavy precipitation. With these similarities, we base the decision on the project with the most cyber components. Therefore, our first case is the GM4W project. There are two projects which regard cybersecurity as 'extremely important'. Of the two cases, one also covers the 'Disasters and ICT' topic. Therefore, our second case is the QoAir project. We continue with a brief insight into the projects' aims and structure of the systems involved.

Table 3.6: Key components in the selected cases

Component	GM4W	QoAir
Data processing/analysis tool	✓	✓
Servers	✓	✓
Anti-virus	✓	✓
Accessible hardware	✓	✓
Human Machine Interface		✓
User Interface	✓	✓
Firewall	✓	✓
Communication line	✓	✓
Offline data storage	✓	✓
Smart meters	✓	✓

3.2.2 The GM4W case

The first case in this study is the GM4W – GeoGuard Module for Water vapor monitoring project. From the database of web content of the Climate Innovation Window, we derive data on the project. The GM4W uses Global Navigation Satellite Systems (GNSS) to monitor water vapor on a local scale to improve both the nowcasting and forecasting of heavy precipitation. The monitoring system is based on the theory of the ground convergence process as a precursor of rainfall. The measurement equipment should identify fluctuations in water vapor near ground level and use the measurement data in prediction models for local heavy precipitation events. The system consists of two main components, the GeoGuard monitoring unit, and the GeoGuard cloud. Two-way communication connects the two components (see Figure 3.3). Figure 3.4 zooms in on the monitoring unit of the system. We identify network access points for the sensors and direct connection through the Ethernet. The system is powered by solar power and through the electricity grid. A local storage unit stores the location and management data. The communication module is center in the system, providing data communication between the system and sensor, while also communicate with the cloud. The cloud provides an infrastructure for the sensing data and translates that data to specific data for the client through an end-user service interface (see Figure 3.5).

A current limitation of the system is the dependency on existing networks of GNSS systems. This limitation might raise complications when deploying the system in developing countries, which have limited networks of GNSS stations. However, the use of these networks ensures low-cost hardware usage of the system. Each sensing unit is collecting raw data, whereas the cloud environment of GeoGuard processes the data. Specialized staff monitors the system and ensures the quality of the end-user service with customized solutions and a help desk service.

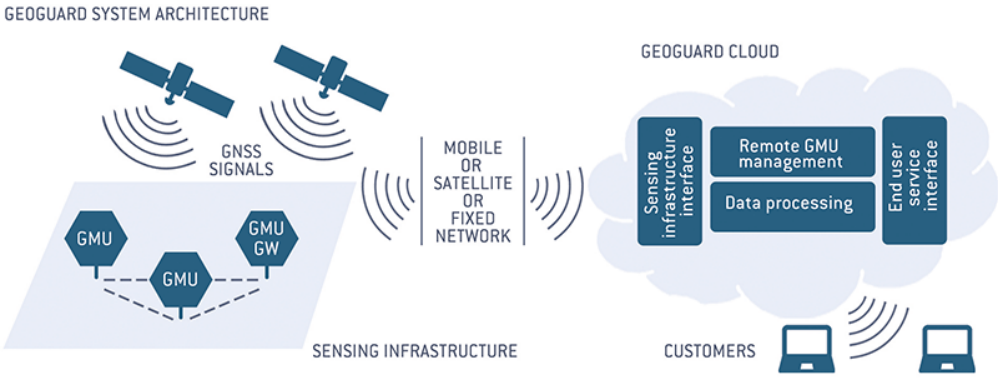


Figure 3.3: GeoGuard architecture (GReD, 2018)

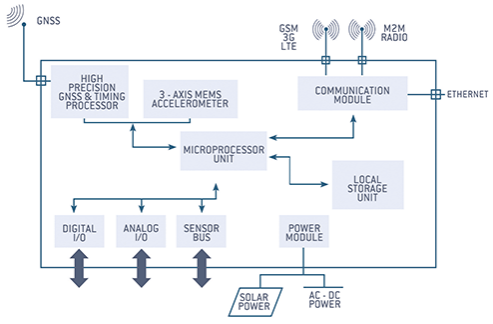


Figure 3.4: GeoGuard GMU (GReD, 2018)

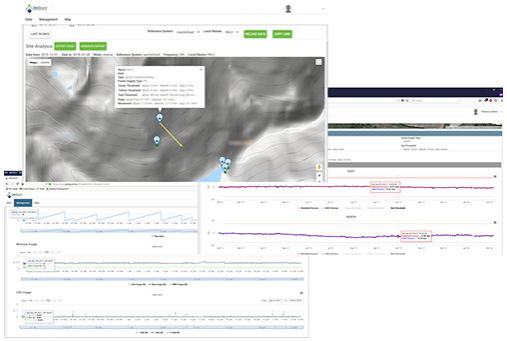


Figure 3.5: GeoGuard Cloud (GReD, 2018)

3.2.3 The QoAir case

Section 1.1 mentions heat waves as one of the most prominent and deadly hazards. The second case for our study aims to mitigate the effects of heatwaves by improving the accuracy of temperature measurement and prediction. QoAir aims at improving temperature measuring and heatwave detection in urban areas. The measuring from apps we have currently are not always accurate. The real degree and real feel of the metropolitan regions differ from the measurements of current equipment. We define the differing local temperature in urban areas as Urban Heat Island (UHI). The heat island is a populated area which has a higher average temperature than the surrounding (rural) area (Environmental Protection Agency, 2014). QoAir is designed to help measure and detect UHIs. Furthermore, the system checks the humidity and air pressure as well, as these measurements relate to heatwaves. The main idea is to build a network of sensors over the entire urban area that is monitored. The network and users connect through a fast and decentralized information system with blockchain technology. The sensor information is synthesized for information purposes, while a trigger detects cases of heatwave conditions in the urban area. The governmental institution of the area will be notified to use guidelines for the preparation of the population against heatwaves. These guidelines are also part of the distributed database within the blockchain and are improved through the blockchain with greater stakeholder involvement and innovative ideas. The system can integrate other users and subsystems to the blockchain in the future.

Different fields of study incorporate the use of blockchain. However, QoAir's use of blockchain technology is a rather new field of research and faces new challenges. The main feature of blockchain technology is the transparency and security of shared information within the system. Improving the information to the community and the countermeasures set out by the governmental institutions will benefit everyone in managing one of the most prominent and deadly hazards we as a society face.

3.3 CHAPTER CONCLUSION

This chapter focused on BRIGAID and the innovation projects linked to the program. The TIF, which we seek to extend, is introduced, and we described the innovation projects. We use two data gathering methods for this analysis. First, we gathered information on the innovation projects from the Climate Innovation Window through web scraping. We use a Python script to visualize and clean up the data and store it into a database. Second, we use a survey to gather data from the innovators on their perception of cybersecurity and the cyber components of their projects' systems. We use the results to identify key cyber components and representative cases for the risk assessments.

We found two innovation projects fit for this study. The first case, GM4W, is a monitoring service system which focuses on the nowcasting and forecasting of heavy precipitation to prepare local entities more accurately on the extreme weather conditions, may these occur. The second case is QoAir, which is a blockchain network of weather measuring sensors. Governments can use this system in urban areas to detect urban heat islands more efficient.

The next chapter presents the review of assessment methodologies found in literature and practice. A risk assessment methodology is selected to follow in this study. In combination with the cyber components from Chapter 2, the methodology is used to assess the selected cases from this chapter.

4 SELECTING A RISK ASSESSMENT METHOD

As introduced in Section 1.2.2, the objective of this study is to assess where in the TIF cybersecurity is relevant and how to assess risks of the projects' systems with this framework. This chapter addresses the question of what risk assessment methodology is available in the literature and which approach is most effective when assessing innovation projects, in this case concerning climate disaster resilience. Section 4.1 will discuss the case-study research approach and how it applies to this research. Section 4.2 will introduce the concept of risk management and definitions of concepts within risk management. After a general conceptualization of risk management, the section will continue discussing the risk assessment concept in greater detail. Next, Section 4.3 discusses the process of finding a risk assessment method with the best fit to the goal of this study, and a general overview of the methodology that we choose to use. Section 4.4 concludes the chapter.

4.1 CASE-STUDY RESEARCH

This study will analyze the two projects selected in Section 3.2 as representative cases for innovation projects. The case study method will be used to structure the research. Gerring (2004) defines a case study as *"an intensive study of a single unit for the purpose of understanding a larger class of (similar) units"* (Gerring, 2004, p.342). The use of cases in this study aims to make generalizable conclusions for the cybersecurity of innovation projects. The cases will be subject to a risk assessment, of which the results are the foundation of the recommendations for the cybersecurity of innovation projects in climate disaster resilience. We use these representative cases to find conclusions on how to identify and mitigate risks effectively, generalized for innovation projects. Generalizing from a limited number of cases may raise concerns about the significance of the results. Yin (2003) counters this concern by distinguishing two types of generalization. Instead of generalizing statistically, where large sample sizes are desirable, we generalize analytically by expanding standing theories and find generalized theories for innovation projects and climate disaster resilience. Yin (2011) structures the case study in a stepwise approach. This study will follow this approach in designing the case study most fitting to the innovation projects and risk assessment methodology (see Figure 4.1).

The first step is the case study design. In this step, we define what a case is in this study, and we select what type of case study to use. Also, we address the use of theory. A case, in this study, is *a single project which is innovative in nature and possesses key cyber components, as defined in this study*. This definition bounds the case within a unique innovation project. We identify key components through the survey in Section 3.2. Results from the survey will be re-examined in the case study and discussed in greater detail. The use of multiple cases, two cases in this study, leads towards a multiple-case design. We assess the two cases in the same manner, which results in an embedded, multiple-case design according to the types of case studies as defined by Yin (2003). We use this type to assess the representative projects individually and compare their results. This approach falls within the lines of a multiple case study, which allows the researcher to examine the similarities and differences between cases (Baxter and Jack, 2008). In terms of the use of theory, we derive data from previous chapters and scientific literature to structure the study. The use of theory does not include the use of a theoretical framework necessarily. Yin (2011) discuss in their case definition that explorative research can be accompanied with the selection of 'special' cases, which are cases that cover, for instance, discoveries or unique subjects. The design of this study is built

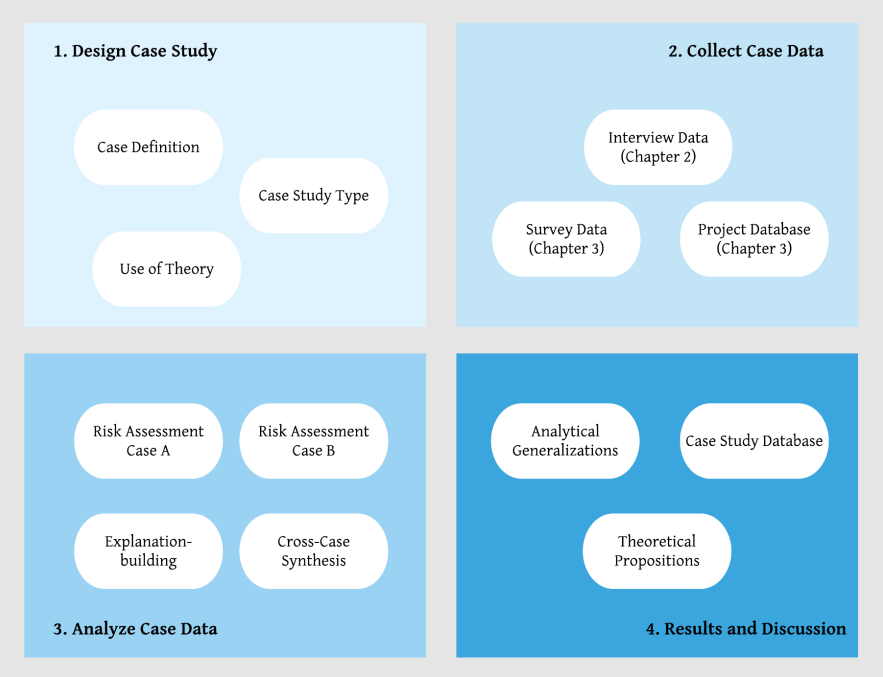


Figure 4.1: The case study design specified for this study, own image derived from (Yin, 2011)

on a theoretical foundation. Additionally, the acquired data from the previous chapters are structured through theory-based methods. However, the explorative nature of this study and innovations as subject to the study ask for a discovery-oriented approach in the execution. The lack of a theoretical framework does not exclude the use of scientific research in the case study. The use of theoretical propositions gives us a direction and to use as starting points of the study. We continue with these theoretical propositions when discussing the data collection in the next step.

Yin (2011) emphasizes the need for multiple sources of data. The previous steps of the research involve both quantitative and qualitative data, which is again used as input to the case study (see Figure 4.1). Additional data is, if needed, collected within the case's environment. The semi-structured interviews in Section 2.3 were semi-structured for the validation of cyber components found in the literature. The open-ended section of the interview is used to derive data on the cases. We collect information on the cases mostly from the innovation project database of BRIGAID (see Section 3.1.3). The database contains data on the projects as provided by innovators to BRIGAID. The survey in Section 3.2 provides quantitative data on the cyber components of the cases' systems. It also provides qualitative data on the perception of cybersecurity within innovation projects.

Following the collection of data, we discuss the analysis of that data. Qualitative data is coded through word tables to derive conclusions. A word table is, in essence, a unique coding mechanism to present and structure the narrative data from interviews (Yin, 2011). We use an explanation building technique for the structure of presenting our conclusions. Data is used to form explanations that were not preceded by (theoretical) predictions at the start of the study. The quantitative data from the survey partly support the risk assessments of the cases. Cyber component information should form the conceptual system of a case, with additional information from the database entry of the project and theory from literature and practice. We compare data from both cases to a so-called cross-case synthesis. As the structure of the cases is the same, we compare the results and identify the similarities and differences.

The last step of the case study, results and discussions, continues with the results from the case studies and the cross-case synthesis of the two cases. The results are used to make analytical generalizations. We discuss the distinction Yin (2003) makes between statistical and analytical

generalization at the beginning of this section. Yin (2011) explains the process of generalizing analytical based on conceptual claims. We claim a theory for the results we find and follow the generalization from there. The claim we make should apply to other situations. An example of analytical generalization is the case study on the funding of Fairfield University, a private college. The found factors of increasing costs and decreasing revenue were analytically generalizable to other private universities of the same size as Fairfield University, as the literature indicates (Tellis, 1997). Besides the theoretical propositions and analytical generalizations, we conclude with a collection of the data from the case study in a database. This collection is the memory of the study, i.e. presenting the data as used in the study ensures reproducibility. Future research can continue or build from this starting point.

4.2 RISK MANAGEMENT

4.2.1 The Concept of Risk Management

Ross (2011) discusses the National Insitute of Standards and Technology (NIST) guide that defines risk management as a comprehensive process that addresses risks throughout an organization. Figure 4.2 shows the four components that form the risk management process. There are several standards and/or guidelines for risk management in sectors concerning information and cybersecurity, such as International Standards Organization (ISO) and NIST (NIST, 2002; Disterer, 2013; NIST, 2011). This section will define risk management according to the NIST guideline components.

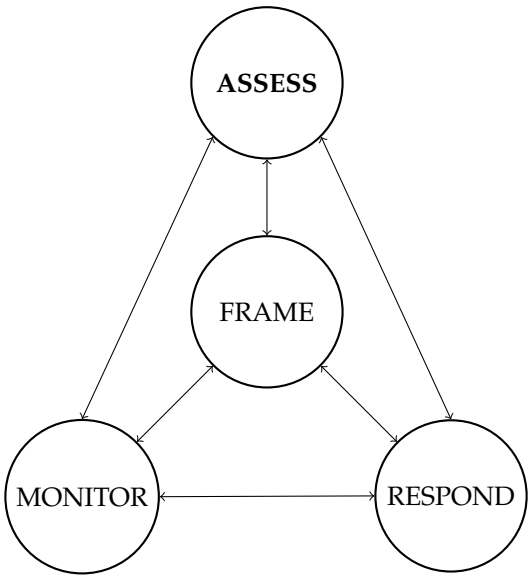


Figure 4.2: Risk assessment within the risk management process, as derived from Joint Task Force Transformation Initiative (2012).

The first component, risk framing, defines the term risk for the managed organizations. We identify what assumptions are made for the threats, vulnerabilities, impact, and likelihood of occurrence when managing risks. Here we identify constraints on the other risk management components. The levels, types, and acceptable degrees for the uncertainty of risks we establish as well. Finally, the priorities and trade-offs made for the different types and levels of risks are also defined. This definition results in a risk management strategy, which serves as the foundation for the other risk management components. This foundation is similar to the framing used in the ISO31000 standard. The scope, context, and criteria are determined first (Purdy, 2010).

The second component is the risk assessment. This component is the main focus of this study. The purpose of the risk assessment is to identify the threats and vulnerabilities to organizations. These threats have a likelihood of occurring, which should be determined

as well. Methodologies and tools from literature support this component, and the framing component establishes the risk management strategy (Ross, 2011). The risk assessment in the ISO31000 standard is similar to the NIST approach. Purdy (2010) defines the risk assessment in three steps, namely risk identification, analysis, and evaluation. The ISO standard will be discussed in more detail in Section 4.2.2.

The third component is the response of organizations to the risks. The purpose of this component is to respond to the assessed risks that are consistently viable throughout the entire organization. ISO defines this as risk treatment. Organizations must identify the resources that are at their disposal to treat the risks. The risks can then be assigned the resources to accept, avoid, mitigate, share, or transfer the risks.

The fourth and final component is the monitoring component. How organizations monitor risks and how to react to changes over time is what is defined here. The monitoring component has to verify the utilization of the planned response measures throughout the organization. Besides the control of the execution of the organization, the responses itself must be under control as well. The goal is to maximize the effectiveness of risk response measures. The organization controls the operating environment as well. The changes of this dynamic environment could shift vulnerabilities and likelihoods of occurrence for risks.

4.2.2 Risk Assessment

As mentioned in Section 4.2.1, this study centers around the risk assessment. With all concepts briefly discussed, this subsection continues to discuss the concept of risk assessment in greater detail. We divide risk assessment into three steps, with the identification of the risks as a first step. Marotta et al. (2013) describe risk identification as the process of finding the risks to the system, list them, and characterize the elements of each risk. The identification of risks starts with the identification and evaluation of the assets that need protection (the Primary and Supporting Asset identification). The risk identification then builds threat scenarios for each of the supporting assets within the considered environment. In this step, all elements, threats, assets, and vulnerabilities are collected to go through the entire assessment. The core where these three elements collide is what we see as risks to the assessed system (Refsdal et al., 2015).

The second step of the assessment process risk analysis. The risk analysis aims to estimate the risk levels, which is the main goal of the risk assessment. We estimate the risk levels based on two other estimates, namely the estimation of the likelihood of cyber-threats to occur and the estimation of the severity of the vulnerabilities that are exposed to those threats. Knowledge on the threat sources, such as their causal relation to the system and its vulnerabilities are used for the estimation of consequences of incidents as well (Refsdal et al., 2015). Two types of analyses can be used here: a quantitative or qualitative analysis. We chose a qualitative approach. Instead of using quantified numbers, risks are assessed subjectively and ranked. The impact inheritance is valued from insignificant to catastrophic, whereas we value likelihood from rare to certain. The reason we chose a qualitative approach is twofold. Firstly, it is desired to go with a quantitative approach, because of the quantified results it provides. People are more inclined to take action when the results indicate that their threat score is 97 out of 100 instead of "Mitigate" on an accept-monitor-mitigate scale. However, studies on risk assessments showed that quantitative approaches often lack validity because of the lack of historic data (Chockalingam et al., 2017; Verendel, 2009). The lack of data results in results overloaded with assumptions and limitations which devalue the results as a whole. Secondly, we assess the framework that is already in place. The TIF is a self-assessment where innovators subjectively assess their innovations. All tests in place are qualitative, what leans us towards a qualitative approach.

The third and last step in the assessment process is risk evaluation, which focuses on the consolidation of the risk analysis results. Different risk levels separate malicious risks from non-malicious risks. For some risks, the estimates of impact and likelihood may be uncertain,

and this uncertainty can affect the risk level or decision-making when treating these risks (Ashibani and Mahmoud, 2017). Some risks may be aggregated to create more certainty and yield a higher combined risk level. This grouping of risks can also be done to separate malicious from non-malicious risks when the treatment approach focuses on one of the two types of risk (Refsdal et al., 2015).

4.3 RISK ASSESSMENT METHOD

4.3.1 Approach

We perform a literature review to find a suitable method for this research. The search is performed across the field of innovation and recent technology, similarly to the review in which we compile the list of cyber components in Section 2.2. Other fields of study, such as IoT, SCADA, and smart technology, are found to have more methods available, and by performing a thorough review, we hope to find the most suitable method available.

First, we compile a list of methods from the search through both SCOPUS and IEEE Xplore. For the Scopus database search, we use the following search query: `("risk assessment"OR "risk analysis") AND ("innovation project")`. We use the same search query in IEEE Xplore, with the use of single quotation marks instead of the double quotation marks as the only modification to the search query. This search leads to respectively 49 and 358 results. Figure 4.3 shows the process of the literature review on the risk assessment methodologies. The results of both database searches lead to the initial filtering. This initial filtering excludes papers that do not meet the demands of this study. The results should be in English, and the review is limited to conferences and peer-reviewed journals. We use no time confinement in this literature review. There are methods based on standards and guidelines that we established earlier, but recent research and analysis modified these methods. Excluding these standards and guidelines would not benefit the quality of the review. The initial filtering leaves us with 43 paper from the Scopus search and 325 papers from the IEEE search. These results are subject to qualitative filtering. This qualitative filtering must exclude papers that do not cover the necessary method or cover a subject that is unrelated to this study. Scopus has a filter for 'subject area' to filter results for the predetermined subject groups. The subject of these papers, however, is not the main point of interest for this study. We seek to analyze the methodology that is proposed or used in the papers. Papers with using the same method, or a similar version of a method, are filtered to leave us with unique methodologies. We perform the quality filtering of the Scopus results manually by assessing the papers' title, abstract, and keywords. For the IEEE results, we perform the same manual filtering. Before the manual filtering, IEEE has the option to filter the results based on 'index terms', which are key terms of the paper. We excluded papers without either one of the index terms' risk management' and 'risk analysis'. This exclusion lessens the burden of manual quality filtering, which leaves us with 188 results.

In Section 2.2.3, we discuss the results from the study of Jalali and Wohlin (2012), who conclude that database searches and the backward snowballing technique do not outperform one another. Webster and Watson (2002) define a complete and thorough review to be one that does not confine to one methodology. Therefore, we use both methods. The snowballing method initializes from the desk research for Section 1.3. The papers we use in the theoretic conceptualization of risk management and risk assessment in Section 4.2 return in this review.

Table 4.1 shows the number of papers that remain after the initial and quality filtering. The articles resulting from both review methods and filterings are now being compared based on three criteria for this study, which we discuss in the next section. After the screening based on the criteria, we review the remaining papers in greater detail and finally choose a method. Table 4.2 shows the remaining papers that are subject to the criteria filtering. We list the papers by the risk assessment method that they address.

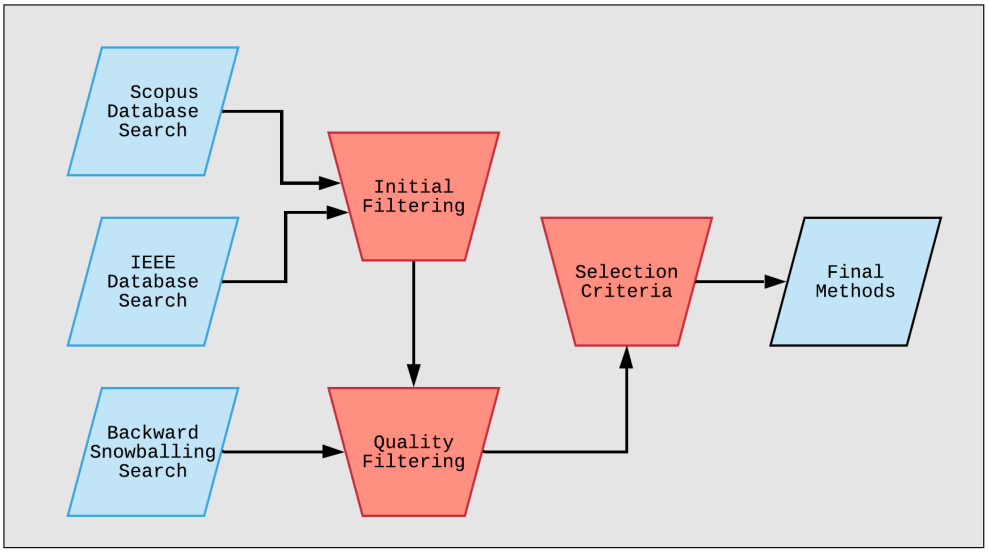


Figure 4.3: Literature review process for the risk assessment methodology

Table 4.1: Results literature review for methodologies

Method	Papers	Papers after filtering	Papers after quality review
Scopus Database	49	43	4
IEEE Database	358	325	4
Backward Snowballing	18	18	13

4.3.2 Selection Criteria

The list of methods will be narrowed down based on three criteria, namely:

C1. Quantitative vs. Qualitative – Risk assessment methodologies divide into quantitative and qualitative methodologies. Quantitative methods measure risks with numerical data and often are probabilistic of nature. Quantitative methods give a clear and direct indication of the level of risk of an assessed system, often by presenting the risks with a percentage or other numerical indication. This indication gives quantitative methods the benefit over qualitative methods by providing numerical values that give an objective indication of the level of risk held by the system. Qualitative methods use a subjective classification of the level of risk in a system. While the objective data of quantitative methods is preferred, the downside of these methods is the need for empirical data. The lack of historical data on cybersecurity issues complicates the use of quantitative models (Chockalingam et al., 2017). The authors, however, argue that the use of Bayesian Networks (BNs) could potentially address this issue thanks to the ability of this technique to effectively use scarce data from different sources. Chockalingam et al. (2017) discuss the need for research on the applicability of BNs for cyber environments. This research is yet to be done and therefore, not considered in this research. Verendel (2009) identified the need for empirical data as a concern for systems' security, as the data is often lacking or incomplete. Furthermore, the lack of data causes the need for assumptions. The author argues that both the empirical data and underlying assumptions lack validity due to little to no empirical validation (Verendel, 2009). This validity issue is of special concern in cybersecurity of innovation, where often historical data is lacking. Assessing innovation systems quantitatively involves complex structures and (relative) new technology. Modeling risks for such complex environments create more difficulties for quantitative methods (Karabacak and Sogukpinar, 2005). We conclude that in the case of innovation projects with limited data available, we qualitatively assess the risks.

Table 4.2: List of considered risk assessment methods

#	Method	Source	Journal	Search Method
1	Common Vulnerability Scoring System (CVSS)	(Mell et al., 2006)	IEEE Security & Privacy	Database
2	Information security risk analysis method (ISRAM)	(Karabacak and Sogukpinar, 2005)	Computers & Security	Database
3	Attack trees	(Byres et al., 2004)	Proceedings of the international infrastructure survivability workshop	Snowballing
4	Probability Risk Analysis (PRA)	(Ralston et al., 2007)	ISA Transactions	Database
5	OCTAVE Allegro	(Caralli et al., 2007)	Software Engineering Institute	Snowballing
6	Knowledge-Based Risk Management	(Alhawari et al., 2012)	International Journal of Information Management	Database
7	Performance-oriented risk management	(Wang et al., 2010)	Technovation	Database
8	Security risk vulnerability assessment	(Farahmand et al., 2003)	Proceedings of the 5th international conference on Electronic commerce	Snowballing
9	Threat metrics and model	(Mateski et al., 2012)	SANDIA National Laboratories	Snowballing
10	Hierarchical homographic modeling (HHM)	(Chittester and Haimes, 2004)	Journal of Homeland Security and Emergency Management	Snowballing
11	Network Security Risk Model (NSRM)	(Henry and Haimes, 2009)	Risk Analysis	Snowballing
12	Vulnerability assessment	(Permann and Rohde, 2005)	Proceedings of the 15th Annual Joint ISA POWID/EPRI Controls and Instrumentation Conference	Snowballing
13	Risk-assessment model for Cyber Attacks on Information Systems	(Patel and Zaveri, 2010)	Journal of Computers	Snowballing
14	Risk Assessment for the design of I & C Systems	(Song et al., 2012)	Nuclear Engineering and Technology	Snowballing
15	Cyber-physical System Risk Assessment	(Peng et al., 2013)	Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing	Database
16	Multicriteria Decision Framework	(Ganin et al., 2017)	Risk Analysis	Snowballing
17	Threat Assessment & Remediation Analysis (TARA)	(Wynn et al., 2011)	Defence Technical Information Center	Snowballing
18	Cyber-terrorism SCADA Risk Framework	(Beggs and Warren, 2009)	Proceedings of the 10th Australian Information Warfare and Security Conference	Snowballing
19	Security risk assessment framework for smart cars using the attack tree analysis	(Kong et al., 2018)	Journal of Ambient Intelligence and Humanized Computing	Snowballing
20	Game theory for cyber-physical risk modeling	(Ashok and Govindarasu, 2015)	Proceedings of the 2015 IEEE Power & Energy Society ISGT Conference	Database
21	Security Risk Assessment Methodology (SecRAM)	(Marotta et al., 2013)	Proceedings of the 2013 International Conference on Availability, Reliability and Security	Database

C2. Categorization by Cherdantseva et al. (2016) – Cherdantseva et al. (2016) created a categorization for risk assessment methods for SCADA systems. Although it was created to facilitate a categorization for SCADA systems due to the difficulty in categorizing these assessment methods, the classification scheme is generic and therefore applicable to other domains. The categorization is divided based on the level of detail and coverage of the assessment methods. Methods assessing the system in great detail focuses on the in-depth activities or components of the system, whereas a low level of details looks at systems on a higher level, or at the process and not necessarily on underlying processes. The level of coverage concerns stages of the risk management that are being covered by the assessment method. Some methods only focus on the identification of threats, or on the mitigation of already identified risks. Figure 3.1 shows the categorization of risk assessment methodologies by Cherdantseva et al. (2016). The guideline methodologies are most fit for the assessment of innovation projects in this study. The level of detail distinguishes two categories, namely elaborated guidelines and guidelines. The elaborated guidelines focus on specific activities in great detail, while also cover all steps of the risk management process. The detail of specific activities is of less of an importance in this study, as we aim to address the full risk management process effectively so that the assessment process can be narrowed down to an extension of the TIF. The use of a guidelines methodology enables us to cover the entire risk management process with little detail on the specific activities. The recommendations from this method should provide references to specific methods to address the identified risk in a more detailed manner.

The ability of guideline methodologies to cover most or all of the risk assessment steps is also important in this study. With the ability to cover all of the assessment steps, we assess projects in different development stages. Section 3.1.1 discusses the different stages in which the innovation projects currently are. The readiness level of a project should not affect the ability to assess the security of that project. Assessing risks through all development stages of innovation is beneficial to the project's success rate (Wang et al., 2010). The categories are abbreviated in Table 4.3 to ASM (Activity-specific methods), GL (Guidelines), and GL+ (Elaborated Guidelines).

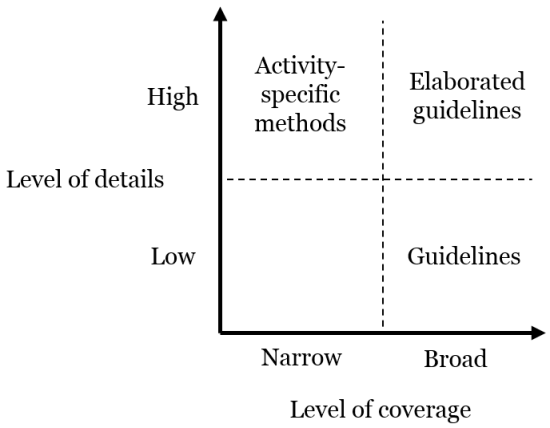


Figure 4.4: Categorization of assessment methods, own image derived from Cherdantseva et al. (2016)

C3. Applicability – The last criterion is a combination of terms tailored specifically to this study. A feature of this research is the projects subject to it. The wide variety of projects that are potential cases in the assessment make it necessary for the method to meet a project's needs. This criterion is comparable to the second criterion, where we discussed the lack of need for a great level of detail, but a need to perform a complete assessment efficiently. The method should, therefore, be modifiable to a project's needs. This rather subjective selection criterion is used to ensure the efficiency of the case study of this research. Case studies and conclusions from papers are used to assess the applicability of a method to the needs of this study. In Table 4.3, a method deemed applicable to this study is marked with a full circle, and marked with semi-circle if it is considered to be partly or somewhat applicable.

4.3.3 Results

The methods following from the literature review are compared based on the criteria discussed in Section 4.3.2. Table 4.3 shows how each of the method scores on the criteria for this study. The first criterion, qualitative vs. quantitative, is given by the methodology part of the studies. In cases where the authors did not specify whether their methodology was qualitative or quantitative of nature, we use our judgment in the analysis of the method. For the second criterion, we use a more subjective approach. Only the papers featured in the review by Cherdantseva et al. (2016) had their category specified before this review. We review the other papers based on the level of details and coverage of the risk assessment steps. Methods which categorize as activity-specific methods have a high level of detail and lack in some part of the risk assessment. Methods tend to focus on a single part of the assessment and execute that in great detail, such as threats (Mateski et al., 2012), vulnerabilities (Farahmand et al., 2003), or risks (Chittester and Haimes, 2004; Henry and Haimes, 2009). Others create risk assessment methods that closely link to the entire risk analysis method, with exclusions to some parts of the analysis (Karabacak and Sogukpinar, 2005; Byres et al., 2004; Wynn et al., 2011). Elaborative guidelines are distinguished from guideline methods by the level of detail. Methods with a dependency on relatively larger sums of data are considered elaborated. Alhawari et al. (2012) combine two methods, both requiring data as input, together to form their method. Their methodology was considered both great in detail and lacking applicability to this study. Wang et al. (2010) had a similar approach with a focus on the level of detail. Their method closely connects to innovation projects. However, their form of innovation projects concerns research and development programs within an organization, which does not account for innovators and independent projects, as found in this study. Therefore this method is considered only partly applicable. The applicability is closely linked to the first two criteria but is unique in valuing the modifiability of methodologies. Peng et al. (2013) serves as an example of a modifiable methodology. Their method is generalizable to projects with cyber-physical assets.

Table 4.3: Criteria covered by risk assessment method

#	Method	C1	C2	C3
1	Common Vulnerability Scoring System (CVSS) (Mell et al., 2006)	Quantitative	GL	
2	Information security risk analysis method (ISRAM) (Karabacak and Sogukpinar, 2005)	Quantitative	ASM	◖
3	Attack trees (Byres et al., 2004)	Qualitative	ASM	
4	Probability Risk Analysis (PRA) (Ralston et al., 2007)	Quantitative	GL+	
5	OCTAVE Allegro (Caralli et al., 2007)	Qualitative	GL	●
6	Knowledge-Based Risk Management (Alhawari et al., 2012)	Quantitative	GL+	◖
7	Performance-oriented risk management (Wang et al., 2010)	Quantitative	GL+	◖
8	Security risk vulnerability assessment (Farahmand et al., 2003)	Quantitative	ASM	
9	Threat metrics and model (Mateski et al., 2012)	Quantitative	ASM	
10	Hierarchical homographic modeling (HHM) (Chittester and Haimes, 2004)	Qualitative	ASM	
11	Network Security Risk Model (NSRM) (Henry and Haimes, 2009)	Quantitative	ASM	
12	Vulnerability assessment (Permann and Rohde, 2005)	Qualitative	GL	◖
13	Risk-assessment model for Cyber Attacks on Information Systems (Patel and Zaveri, 2010)	Quantitative	GL+	
14	Risk Assessment for the design of I & C Systems (Song et al., 2012)	Qualitative	GL	
15	Cyber-physical System Risk Assessment (Peng et al., 2013)	Quantitative	GL+	●
16	Multicriteria Decision Framework (Ganin et al., 2017)	Quantitative	GL+	◖
17	Threat Assessment & Remediation Analysis (TARA) (Wynn et al., 2011)	Qualitative	ASM	
18	Cyber-terrorism SCADA Risk Framework (Beggs and Warren, 2009)	Qualitative	GL	
19	Security risk assessment framework for smart cars using the attack tree analysis (Kong et al., 2018)	Quantitative	GL+	
20	Game theory for cyber-physical risk modeling (Ashok and Govindarasu, 2015)	Quantitative	GL+	
21	Security Risk Assessment Methodology (SecRAM) (Marotta et al., 2013)	Qualitative	GL	●

The blue highlighted cells represent the desired options for this study
C1: Qualitative = Qualitative risk assessment, Quantitative = Quantitative risk assessment
C2: GL = Guidelines method, GL+ = Elaborated Guidelines method, ASM = Activity-specific methods
C3: ● = Applicable to this study, ◖ = partly or somewhat applicable to this study

Two methods scored positive on all criteria, meaning these are qualitative, guidelines methods with an efficient risk assessment process applicable to the cases in this study. The adoption of the OCTAVE method by Caralli et al. (2007) and the application of the Security Risk Assessment Methodology (SecRAM) methodology by Marotta et al. (2013) are more extensively reviewed to pick one of the two options for this study. The OCTAVE Allegro method uses a systematical approach in identifying risks to the system. Worksheets are used to identify a single risk. The number of worksheets used in this method was found to be conflicting with the time constraint of a research (Ali and Awad, 2018). Marotta et al. (2013) used the SecRAM methodology in a cloud-based environment. They concluded that applying the method in another context should be a target for future work. Asgari et al. (2018) applied the method to a system in a recursive internetwork architecture (RINA) environment. The authors tailored the method to the needs of the RINA environment by adjusting the impact assessment (Asgari et al., 2018). The different applications showed that the SecRAM method could be applicable to other fields of study as well. With the broad variety in innovation projects, we prefer a widely applicable method over the use of several preset worksheets as in the OCTAVE Allegro method. Therefore, we follow the SecRAM methodology in the risk assessments of this study.

4.3.4 SecRAM Methodology Overview

The SESAR Joint Undertaking program developed the SecRAM methodology (SESAR, 2013). The methodology follows the ISO 27005 information security risk management. ISO 27005 is a standard methodology to assess the risks of an organization's information (Bahtit and Regragui, 2013). The strengths (S), weaknesses (W), opportunities (O), and threats (T) of the ISO 27005 standard are presented in Figure 4.5. The SWOT matrix shows several strengths that the standard has as risk management. The flexibility and reusability of the standard make it modifiable, leading to methodologies based on this standard, such as SecRAM. This modifiability is needed for the standard to be used in practice, as the weakness shows that the standard does not provide a specific methodology. Bahtit and Regragui (2013) list the lack of experience and practice of the standard as a threat. Marotta et al. (2013) touch on this threat in their reflection, as their recommendation for future work is to test the methodology in other fields of study to examine the applicability. This study tests the methodology in another field of study, as SecRAM initially was for Air Traffic Management (ATM) systems.

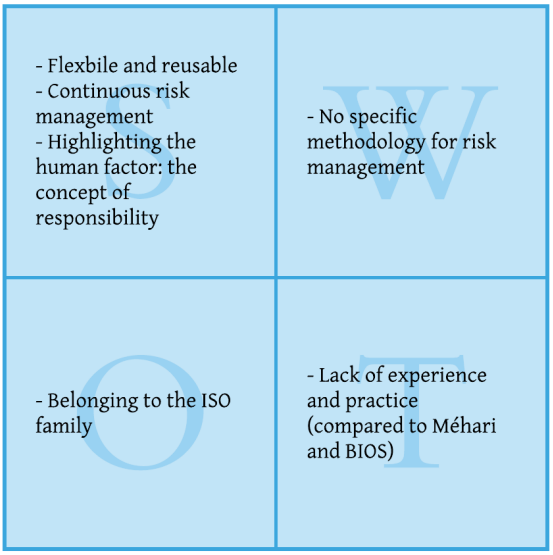


Figure 4.5: ISO 27005 SWOT Matrix (Bahtit and Regragui, 2013, p.532)

The SecRAM risk assessment starts from a context establishment. The scope of the system that is subject to the assessment is vital, what we want to analyze can be set within boundaries and criteria to provide results that are consistent with our initial intentions for the assessment (Asgari et al., 2018). The methodology follows a standard procedure for risk assessment and treatment (see Figure 4.6).

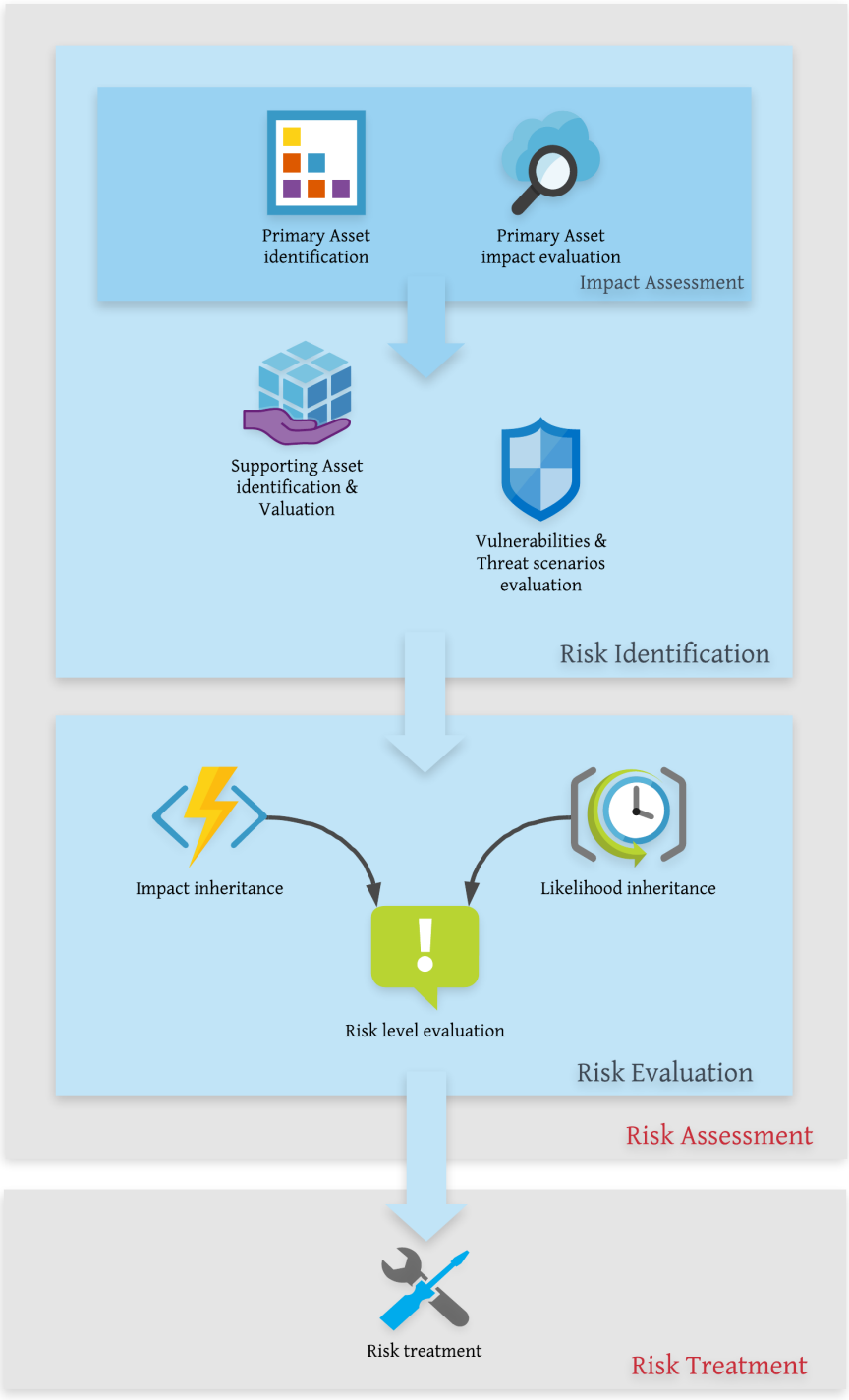


Figure 4.6: SecRAM Methodology, adapted from Marotta et al. (2013, p.808)

The first step of the assessment itself (excluding setting the context and scope) is the identification of assets. The SecRAM method identifies two types of assets, namely Primary Asset (PA)s and Supporting Asset (SA)s. PAs are the information and services provided by the assessed system. The assets highlight the importance of the context and scope of the assessment. We

find various sources for information suppliers and service providers. The question is, which are part of the system within our scope. These PAs are intangible, i.e. assets that are not physical and therefore need a tangible asset to enclose them. These are the SAs, which in this study resemble the cyber components as discussed in Section 2.2. The PAs are identified first, after which we assess the impacts that attacks on these assets can bring to the system. We follow the CIA principle when assessing the impact. The CIA consists of three levels of affection to an asset:

- **C** - The level of confidentiality determines how the system discloses information and services. Unauthorized entities should not have access to the asset, as these entities can use the asset for other, potentially harmful, purposes
- **I** - The level of integrity is a safeguard of the accuracy and completeness of the information and services provided. Modified or malicious information and services damages processes or the system in its entirety
- **A** - The level of availability is the continuous access for authorized entities upon demand. Limited availability may harm the continuation of the system and its processes

The impact of an attack on each primary asset will be assessed on a one-to-five scale according to the loss of CIA in different Impact Areas (IA) (see Table 4.4).

After the impact assessment, supporting assets link with the primary assets they encapsulate. The linkage of SAs and PAs is the preliminary step to the threats and vulnerability identification. Table 4.5 shows the structure of this step. The first column lists the supporting assets, with threats identified for the SA. These threats come from a particular vulnerability to the assets, which is listed next to the threat. Next, we have the primary asset that links to the supporting asset with their overall impact value for the CIA levels. Threats do not necessarily include all three levels. On the contrary, most often, a threat only affects a primary asset on one of the three areas. The threat inherits the overall impact of the corresponding CIA levels of the affected PA.

In the next step of the assessment process, the maximum value that a threat inherits from the primary asset is the inherited impact of that threat. The SecRAM method also has a reviewed impact. The reviewed impact is a mean to define impacts that are known, and a mitigation strategy is already in place in the system. For this study's focus on innovation projects, we choose to refrain from using reviewed impact and work with the inherited impact for the threats. This choice ensures the applicability to all potential projects and consistency in the results, i.e. the same impact is used in all projects, instead of some projects working with reviewed impacts and relative unknown innovations having to work with inherited impact.

After the impact of the threat, we assess the likelihood of the threat to occur. The likelihood score is also on a five-point scale, ranging from an improbable chance of occurrence to a frequent occurrence (see Figure 4.7). With both the impact and likelihood, we can calculate the risk level according to the equation risk equals the impact multiplied with the likelihood of occurrence. Figure 4.8 shows the risk levels as a product from the impact and likelihood values. We use the compiled list of risks for the final step of the method: the risk treatment.

In the final step of the methodology, we focus on the treatment of found risks. The level of risks determines how we treat the risks. We distinguish three levels of risks, low, medium, and high. Each of the three risk levels has its managing decision. We derive the decision options from Blakley et al. (2001), who define four mechanisms for risk management. Table 4.6 presents the managing option for each of the risk levels.

The first option, liability transfer, is not linked to a risk level. With this option, the subject of the assessment handles the risk, no matter what level, by transferring the liability to another entity. We do this either by entering an activity with the explicit understanding that the subject

Table 4.4: Classification per impact area, adapted from Marotta et al. (2013)

	5	4	3	2	1
Impact Areas (IA)	**Catastrophic**	**Critical**	**Severe**	**Minor**	**No impact / NA**
IA1: Personnel	Fatalities	Multiple severe injuries	Severe injuries	Minor injuries	No injuries
IA2: Capacity	Loss of 60%-100% capacity	Loss of 30%-60% capacity	Loss of 10%-30% capacity	Loss of up to 10% capacity	No capacity loss
IA3: Performance	Major quality abuse that makes multiple major systems inoperable	Major quality abuse that makes major system inoperable	Severe quality abuse that makes systems partially inoperable	Minor system quality abuse	No quality abuse
IA4: Economic	Bankruptcy or loss of all income	Serious loss of income	Large loss of income	Minor loss of income	No effect
IA5: Branding	Government & international attention	National attention	Complaints and local attention	Minor complaints	No impact
IA6: Regulatory	Multiple major regulatory infractions	Major regulatory infractions	Multiple minor regulatory infractions	Minor regulatory infractions	No impact
IA7: Environment	Widespread or catastrophic impact on environment	Severe pollution with long term impact on environment	Severe pollution with noticeable impact on environment	Short term impact on environment	Insignificant

Table 4.5: Vulnerabilities and threat evaluation

Supporting Assets (SA)	**Threats**	**Vulnerabilities**	**Primary Assets (PA)**								
			PA1			*PA2*			...		
			C	I	A	C	I	A	C	I	A
		Overall Impact ⇒									
	Threat A										
SA1	Threat B										
	Threat C										
	Threat X										
SA2	Threat Y										
	Threat Z										
...	...										

Likelihood	**Qualitative and quantitative interpretation**
5. Frequent	high chance that the scenario occurs in a short term
4. Probable	high chance that the scenario occurs in a medium term
3. Occasional	high chance that the scenario occurs during the life time of the project
2. Remote	a low chance that the scenario occurs during the life time of the project
1. Improbable	very little/no chance that the scenario occurs during the life time of the project

Figure 4.7: Likelihood scale

	Impact				
Likelihood	1	2	3	4	5
5	Low	High	High	High	High
4	Low	Med	High	High	High
3	Low	Low	Med	High	High
2	Low	Low	Low	Med	High
1	Low	Low	Low	Med	Med

Figure 4.8: Risk levels

Table 4.6: Risk management strategy per risk level

Risk Level	Management Strategy
-	Liability transfer
Low	Retention
Medium	Mitigation
High	Indemnification

cannot be held accountable to the consequences or by agreeing with a counterparty upfront on them being responsible for the consequences in case of the threat occurrence.

The low-risk treatment is 'retention', where the subject accepts the risk and its implications or accounts for the (inevitable) occurrence of that risk. Blakley et al. (2001) use the example of businesses accounting for lean years by building a fund in years where they make substantial profits.

With medium risks, we use mitigation as treatment. Reducing the expected costs of a risk occurrence mitigates risks. Here we use the pre- and post-controls for risk treatment. Pre-controls are controls that benefit the system by lowering the chances of a risk to occur. The system is re-designed or adjusted to fix issues that cause the likelihood to occur. Post-controls are controls that lower the impact by improving the system with measurements that reduce the effects of an occurred risk.

Lastly, there is 'indemnification' for high-level risks. Blakley et al. (2001) distinguish two types of indemnification, namely pooling and hedging. In pooling, often unlikely events with a high impact can harm a 'pool' of entities with shared environments of their systems. By forming a pool and sharing the risks, the high costs are spread out among the pool, while it protects everyone from paying those costs on its own. A prime example of a risk pool is an insurance policy. Hedging is another type of cost-sharing. The system which bears the risk offers other entities funds to share the risk. The other entities get refunded if a risk does not occur over a specified period. In the case where the risk does occur, the system can use the funds from other entities to cover the costs of the risk. In this study, the managing of the risk is limited to the management type, i.e. the type of risk treatment will be presented, but we will not work out entire risk managing strategies, as this falls out of the scope of the research.

4.4 CHAPTER CONCLUSION

This chapter addressed the question of what research methods are available and relevant to this study. We found the case study to be most fitting to the study due to the exploratory nature of the research and innovation projects in general. A stepwise approach was used to structure the case study design, and we chose an embedded, multiple-case study as the type of case study. The cases' definition is a unique innovation project with key cyber components that will be subjected to risk management. We use data from interviews, the project database, and the survey for the assessments.

After a thorough literature review, we found the SecRAM methodology most fitting to the needs of this study. We will use this method for the risk assessments, and eventually to help design the extension to the TIF of BRIGAID. The next chapter will present the results of this study. The data from previous chapters will be used to perform the case studies, as discussed in this chapter.

5 RESULTS

This chapter presents the results of this study. We present the case studies of the innovation projects in the form of risk assessments. We use the gathered data from the previous chapters in the case study. The cyber components and expert interview data of Chapter 2, along with the database of the climate innovation window and survey results of Chapter 3 are featured in the risk assessments. First, we present the results of the two risk assessments in Section 5.1 and Section 5.2. Second, we analyze the results from the risk assessments in a cross-case synthesis (Section 5.3). As we assess the cases in the same structure, we can compare results and present identified similarities and differences. Lastly, Section 5.4 summarizes our findings and concludes the chapter.

5.1 RISK ASSESSMENT GM4W

Section 3.2.2 briefly presents the system of GM4W. This section presents the project's system in the perspective of the SecRAM, i.e. focusing on the primary and supporting assets of the system. Figure 5.1 shows the system of GM4W according to the identified primary and supporting assets. The dashed line distinguishes the GeoGuard Measurement Unites (GMU) on the left from the cloud environment on the right.

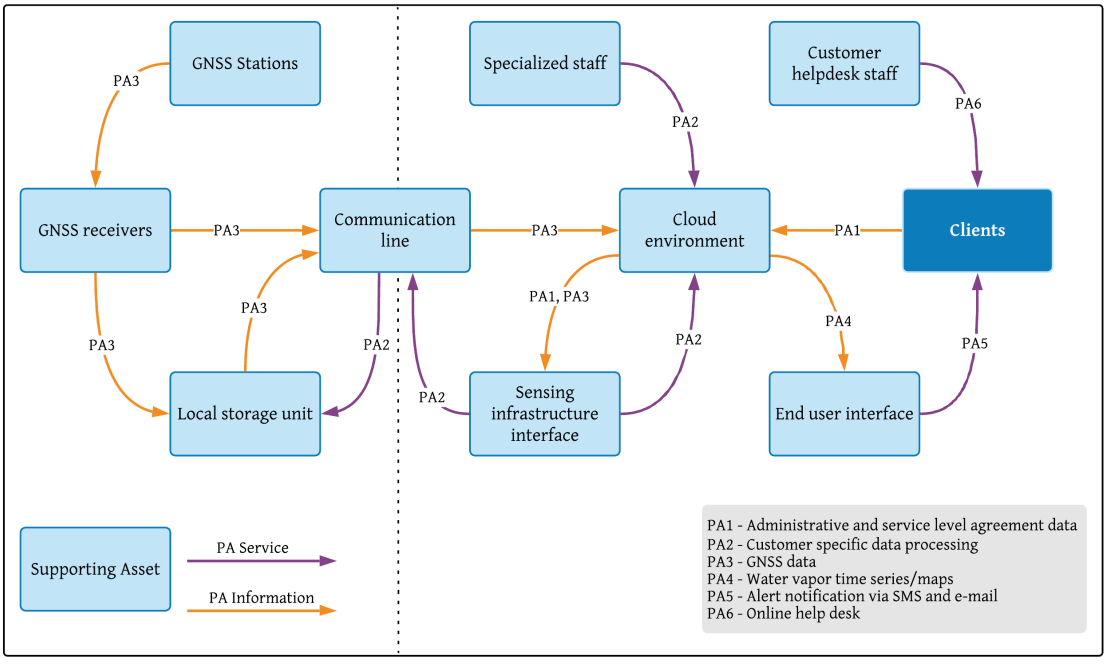


Figure 5.1: System diagram of GeoGuard, derived from Figures 3.3 and 3.4 and GReD (2018)

Step 1 Primary Assets - The primary assets are the intangible products of the system that are valuable and prone to cyber threats (see Table 5.1). The first primary asset (PA1) is the administrative and service level agreement data. This asset involves the client-specific data that the system uses for local measurement unit deployment, fit to the needs of the client. The cloud sends this data to the sensing infrastructure interface, where this customer-specific data is processed (PA2) and used to derive the needed raw data from the GNSS data (PA3). GNSS stations send the data to receivers on location, which transmit real-time data to the cloud or store the data in the local storage unit. A specialized staff monitors the processes within the cloud to ensure that the end-user interface has the right information in the form of water vapor time series and maps (PA4). Within this interface, clients can see their model, and the system sends an alert notification via SMS and e-mail (PA5) in case of heavy precipitation chances. The system also has a staff to resolve issues clients may endure through an online help desk (PA6).

Table 5.1: Primary Assets of the GM4W case

PA #	Name	Type
PA1	Administrative and service level agreement data	Information
PA2	Customer specific data processing	Service
PA3	GNSS data	Information
PA4	Water vapor time series/maps	Information
PA5	Alert notification via SMS and e-mail	Service
PA6	Online help desk	Service

Step 2 Impact Assessment - This step determines the impact a potential compromise of a primary asset can have on seven impact areas. The primary assets have three affections, namely confidentiality, integrity, and availability. Table 5.2 shows the justification of the impact per potential compromise. The table also presents the impact score per impact area. Here, we discuss the overall impact on each area if a compromise would occur:

Personnel: In this system, the personnel is not in any danger, and compromise of the system would not lead to any physical injuries to the personnel. Therefore, we value the overall impact on this area with one out of five.
Capacity: The capacity of the system can be impacted by risks occurring. Due to the split between data gathering and data processing systems, a compromise of either system would lead to a full capacity loss. Neither of the systems can run independently. Therefore, we value the overall impact on this area individually per compromise.
Performance: The performance of the system is highly sensitive to risks. As mentioned in the capacity impact area, the systems work in series and are dependent on one another. Quality abuse would lead to full inoperability of all systems. Therefore, we value the overall impact on this area individually per compromise.
Economic: The project earns from monitoring water vapor data points, and missing these points results in a loss of income. The monitoring side of the system is specific to the client's location and only affects the service to that client. The cloud side is center in the system and affects all clients, resulting in a loss of all income if the cloud is not operating. Therefore, we value the overall impact on this area as no effect (1), a large loss of income (3), or loss of all income (5).
Branding: The impact on the reputation can be significant if the system misses too many water vapor points. A single miss can have an impact on the client, but structural misses can lead to mistrust across the board of clients, impacting the reputation on a larger scale. Therefore, we value the overall impact on this area individually per compromise.
Regulatory: Continuous misuse of client data and the inaccurate result may cause regulatory infractions. Additionally, the use of GNSS data can be subject to infractions as well. Potential infractions are minor of nature. Therefore, we value the overall impact on this area individually per compromise between 1 and 2.
Environment: The primary assets of GM4W's system do not affect the environment to the ex-

tent of at least short term impact, making the potential impact insignificant. Therefore, we value the overall impact on this area with a 1 out of 5.

Table 5.2: Impact assessment of the GM4W system

PA	Compromise	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact	Justification
PA1	C	1	1	1	1	2	2	1	**2**	The agreement between the project and the client should be kept in between the parties, as the data may contain sensitive information on the system's service and/or the client's assets
	I	1	3	2	1	3	1	1	**3**	The data from the agreement is input for the client-specific processing of data. Inaccurate data results in a monitoring system which potentially does not serve the client or provides wrongful data
	A	1	2	2	1	2	1	1	**2**	The availability is only an issue at the start of the agreement, where the client-specific system is designed and for the specialized staff to monitor the performance of the system
PA2	C	1	1	1	1	2	2	1	**2**	Contains data specific to the client, which may concern sensitive data to that client. Data should be kept within the boundaries of the system
	I	1	1	3	3	3	1	1	**3**	The process of producing models specific to the clients is crucial to the perception of the client on the performance of the system. Inaccurate data may lead to errors in the model or wrongful results
	A	1	3	4	3	3	1	1	**4**	The processing step is crucial to the performance of the system. Without this process, the system works solely with the raw data from the GNSS data gathering
PA3	C	1	1	1	1	1	2	1	**2**	GNSS data is open source in the sense that every receiver unit can receive information from the various GNSS stations. The data that is received is not sensitive to privacy or other threats
	I	1	3	4	3	3	1	1	**4**	The accuracy of the GNSS data is crucial to the system's innovativeness and core purpose of providing accurate nowcasting and forecasting data
	A	1	5	5	3	3	1	1	**5**	The availability of GNSS data is crucial in the sense that loss of data results in inaccurate data. The system relies on up to date data as input to the prediction models
PA4	C	1	1	1	1	2	1	1	**2**	Customer-specific data which can contain sensitive data on operation location and client needs
	I	1	4	5	5	3	1	1	**5**	The accuracy of this end product is vital in the customer satisfaction and effectivity of the model predictions
	A	1	4	5	5	3	1	1	**5**	The availability of the end product is crucial to the customer's rating of the service, downtime defeats the purpose of the system
PA5	C	1	1	1	1	1	1	1	**1**	Data is not sensitive and can even benefit other entities. However, alerting system should send out messages to at least the clients who are depending on the system
	I	1	1	2	1	3	1	1	**3**	Alerting notifications should be accurate to secure the production of the system. False alarms and missed events greatly decrease the clients' trust in the system
	A	1	1	2	3	3	1	1	**3**	No alerting notifications refrain the system from meeting its purpose, the alerting mechanism should be at least stand-by at all times
PA6	C	1	1	1	1	1	1	1	**1**	Help desk service can be openly accessible, non-clients should not have access
	I	1	1	1	1	2	1	1	**2**	An accurate and complete service benefits the customer satisfaction, yet not crucial for the system's operations
	A	1	1	1	1	2	1	1	**2**	The customer service desk should be available at the convenience of the clients, not critical for the operations

Step 3 Supporting Assets - In this step, we connect the primary assets to supporting, tangible assets. The supporting assets are the cyber components relevant to the risk assessment of the system. Table 5.3 presents the supporting assets and corresponding cyber components. The staff assets are an exception, as they do not resemble a single component. The staff members are part of the roles and responsibilities element we discuss in Section 2.1. The human roles are not encompassed by the cyber component but do make use of components, such as *'data processing/analysis tools'*, *'human machine interface'*, *'servers'*, and *'accessible hardware'*. Figure 5.1 shows the connections between the supporting assets and the primary assets that they affect. We present these relations in the supporting asset table with a 'x' (see Table 5.3).

The GNSS stations send the GNSS data to the receivers. Real-time data is sent directly to the cloud via the communication line. The local storage unit stores other information from the GNSS infrastructure. The administrative and service level agreement data comes from the agreement between GReD and its clients. The cloud receives specific data and processes it across the system. Both the specialized and help desk staff can access this information to provide their services. The specialized staff monitors the client-specific data process, while the help desk staff offers a service in the form of an online help desk for the clients. The sensing infrastructure interface uses the same information to process data into water vapor time series/maps, specific to the clients' needs. The client-specific data processing facilitates this information, which takes place in the cloud between the sensing infrastructure interface and the end-user interface. The alert notification following from the models in case of heavy precipitation are sent out through the end-user interface to the clients. The end-user interface receives the necessary information from the cloud.

Table 5.3: Supporting Assets of the GM4W case

Cyber Component	**Supporting Assets / PAs**	PA1	PA2	PA3	PA4	PA5	PA6
Communication	GNSS stations			x			
Sensors	GNSS receivers			x			
Offline data storage	Local storage unit			x			
Communication line	Communication line			x			
Cloud technologies	Cloud environment	x	x	x	x	x	
Real-time data	Sensing infrastructure interface		x		x		
User Interface	End user interface	x			x	x	x
	Specialized staff	x			x		
	Customer help desk staff	x					x
Accessible hardware	Power source		x	x	x	x	x

Step 4 Threats - We identify threats according to the supporting assets. We discuss the identified threats in this step and present them in Table 5.4. GNSS satellites and receivers are prone to two types of attacks, namely signal jamming and signal spoofing. The jamming of the signal complicates the communication between the two supporting assets. The spoofing modifies communicated data.

Data stored on hardware is vulnerable to data loss due to factors such as hardware failure, insufficient storage space, malware, and human errors. Fatal loss of data should be avoided by mitigating these risks.

CIOReview (2016) discusses the risks of cloud and local storages. The cloud provides an efficient way to store data and retrieve it faster when needed. The data is safer in terms of backup in case of disasters. However, new kinds of risks are involved with this technology. It's the user's responsibility to find the right cloud service for the projects and how to backup the data. The databases must be kept up to date and encrypted to ensure safety. Data on the cloud faces numerous threats. Data can become prone to hackers or other types of cyber attackers, who can either access the cloud from within the company or directly attack the cloud server. Another threat comes with the cloud services, which can temporarily or even permanently become unavailable due to connectivity issues or problems with the supplier. That brings us to the final treat, which is vendor lock-in. Vendor lock-in is a concept where the customer is unable to switch vendors to supply products. In this case, some vendors protect themselves from the competition by making it difficult for the customer to transmit their data through a different service.

Within the system, we have different types of staff. The specialized staff must monitor the processes within the cloud to ensure the quality of the client-specific information. This quality control requires access to all of the information and services in the system. We distinguish two types of threats when assessing staff, namely human errors and insider attacks. The customer help service staff has the same threats facing the system as the specialized staff. The main difference here is the access to information and services. Where the specialized staff has full access, the help desk staff has limited access to the system.

The power source, either solar power or the conventional electrical grid, can be a threat when unable to provide power to the system. The power architecture should identify the part of the system most at risk in case of a power outage.

Step 5 Likelihood Evaluation - We estimate the likelihood of risk for occurring during the lifetime of a project on a one-to-five scale. We find the estimation by taking into account what assets a person would need to attack the system, as seen in Marotta et al. (2013). We account for the time and skills the attacker need for a successful attack. Besides overall time and skill, the attacker needs specific knowledge of its target, and the target needs to be available for an attack. Table 5.5 presents the score of the threats on each of the likelihood measures and the overall likelihood scores. Most likely threats to occur are human errors and power outage.

Table 5.4: Threats for the GM4W system

Supporting Assets	Threats	Primary Assets PA1 C	PA1 I	PA1 A	PA2 C	PA2 I	PA2 A	PA3 C	PA3 I	PA3 A	PA4 C	PA4 I	PA4 A	PA5 C	PA5 I	PA5 A	PA6 C	PA6 I	PA6 A	Impact
	Overall impact ⇒	2	3	2	1	3	3	2	3	4	2	4	5	1	2	2	2	5	5	
GNSS receivers	Signal jamming												x							5
	Signal spoofing											x								4
	Hardware failure												x							5
	Theft										x		x							5
Local storage Unit	Malware										x	x								4
	Hardware failure												x							5
	Theft										x		x							5
Communication line	Signal jamming												x							5
	Signal spoofing											x								4
Cloud environment	Hacking	x						x			x						x			2
	Service denial			x			x			x			x						x	5
	Vendor lock-in	x																		2
Specialized staff	Human error	x	x														x	x		5
	Inside attack	x	x	x													x	x	x	5
Help desk staff	Human error	x	x											x	x					3
	Inside attack	x	x	x										x	x	x				3
Power source	Power outage						x			x			x			x			x	5

These threats were found to be possible threats to occur more frequently than once in the project's life cycle.

Table 5.5: Likelihood of the threats for the GM4W system

Supporting Assets	Threats	Time	Knowledge	Target	Availability	Likelihood
GNSS receivers	Signal jamming		x		x	**3**
	Signal spoofing	x	x	x		**3**
	Hardware failure				x	**3**
	Theft	x	x	x	x	**2**
Local storage Unit	Malware	x	x	x		**2**
	Hardware failure				x	**3**
	Theft	x	x	x	x	**2**
Communication line	Signal jamming		x		x	**3**
	Signal spoofing	x	x	x		**3**
Cloud environment	Hacking	x	x	x		**2**
	Service denial			x		**3**
	Vendor lock-in				x	**2**
Specialized staff	Human error			x	x	**4**
	Inside attack			x		**2**
Help desk staff	Human error			x	x	**4**
	Inside attack			x		**2**
Power source	Power outage				x	**4**

Step 6 Risk Level Evaluation - With the impact and likelihood scored in the previous steps, we can estimate the risk level. Table 5.6 presents the risk level for each threat. The level of risk determines the mitigation strategy in the next step.

Table 5.6: Risk level evaluation of the GM4W system

Supporting Assets	Threats	Impact	Likelihood	Risk
GNSS receivers	Signal jamming	5	3	High
	Signal spoofing	4	3	High
	Hardware failure	5	3	High
	Theft	5	2	High
Local storage Unit	Malware	4	2	Medium
	Hardware failure	5	3	High
	Theft	5	2	High
Communication line	Signal jamming	5	3	High
	Signal spoofing	4	3	High
Cloud environment	Hacking	2	2	Low
	Service denial	5	3	High
	Vendor lock-in	2	2	Low
Specialized staff	Human error	5	4	High
	Inside attack	5	2	High
Help desk staff	Human error	3	4	High
	Inside attack	3	2	Low
Power source	Power outage	5	4	High

Step 7 Risk Treatment - The mitigation strategies for each threat is presented in Table 5.7. Signal jamming (including service denial) and spoofing are high-risk threats on the transmission of data. We assess the transmission of data in the system as critical for the process. Ruegamer and Kowalewski (2015) proposes countermeasures for the jamming and spoofing attacks on GNSS receivers. The countermeasures involve integrity monitoring and detection of signals, encrypting the data, and the prioritization of critical receivers. For the cloud and local storage, we found similar countermeasures. CIOReview (2016) discusses the countermeasure of data encryption and backup protocols for both the local storages and cloud environments. The three main principles for cloud threat mitigation are: data encryption, backup maintenance, and trusted cloud service provider. The interfaces for the sensing infrastructure and end-users merge with the cloud in the assessment of threats. The interfaces are operating in the cloud environment, and the cloud grants access to the interfaces. Building a robust network ensures the continuation of the process in case of incidents. Setting up a backup protocol to ensure the continuation of the processes is a good business case in itself (Information Security Officer, ABN Amro, 2019). Timely backup is the primary mitigation strategy. The backups should follow a periodical protocol with everyone involved strictly following it.

This protocol also applies to the power outage threat. The dependency of power to this system complicates the mitigation of this threat. Using backup generators is a way to ensure the system's continuation. A way to address the limited capacity of generators is to prioritize critical assets (Castillo, 2014). Identifying the critical system of assets mitigates the threat of power outage. These assets require priority when the power supply is limited or in case of a short duration event. Hardening components of the system can achieve the robustness of a system and the prioritization of critical assets. Hardening the system involves closing the network of the system down to only those components and assets that are necessary for the continuation of the system's processes. Everything else should be either removed or secluded from the system (Information Security Officer, ABN Amro, 2019).

Human threats involve theft, insider attacks, and human errors from staff members. The first mitigation step here is identity and access. Identity and access are about the process of defining and controlling which entities have access to what assets of the systems (Information Security Officer, ABN Amro, 2019). The system should monitor who accesses what information and whether this person is allowed to do so. Training the staff mitigates human errors

to some extent, using a backup to create a robust system in case of incidents also can achieve this mitigation.

Table 5.7: Risk treatment for the GM4W system

Supporting Assets	Threats	Mitigation Strategy	Pre-controls	Post-controls
GNSS receivers	Signal jamming	Indemnification	Robust network	Prioritize critical assets
	Signal spoofing	Indemnification	Integrity monitoring	
	Hardware failure	Indemnification	Data encryption, backup protocol	
	Theft	Indemnification	Data encryption, backup protocol	
Local storage unit	Malware	Mitigation	Data encryption	
	Hardware failure	Indemnification		backup protocol
	Theft	Indemnification	Data encryption	backup protocol
Communication line	Signal jamming	Indemnification	Robust network	Prioritize critical assets
	Signal spoofing	Indemnification	Integrity monitoring	
Cloud environment	Service denial	Indemnification	Data encryption	backup protocol
Specialized staff	Human error	Indemnification	Staff training	backup protocol
	Inside attack	Indemnification	Identity and access control	
Help desk staff	Human error	Indemnification	Staff training	backup protocol
Power source	Power outage	Indemnification	Power architecture assessment	Prioritize critical assets

5.2 RISK ASSESSMENT QOAIR

Section 3.2.3 briefly presents the system of QoAir. This section presents the project's system in the perspective of the SecRAM, i.e. focusing on the primary and supporting assets of the system. Figure 5.2 shows the system of QoAir according to the identified primary and supporting assets. The dashed line distinguishes the block chain environment on the left from the system's communication with governmental agencies and citizens on the right.

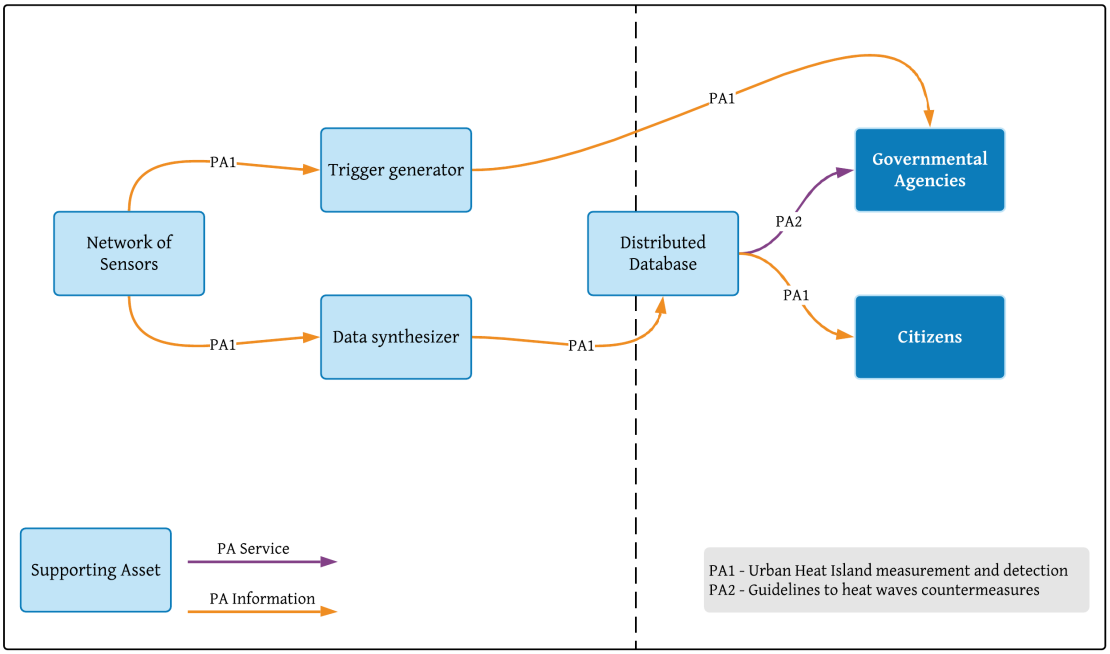


Figure 5.2: System diagram of QoAir, derived from data in the Climate Innovation Window

Step 1 Primary Assets - QoAir provides a couple of Primary, intangible assets. First, we have the information from the sensor network on the temperature and other weather related measurements (PA1). The data from this assets is used to determine whether there is an UHI in the environment of the sensors. The other primary asset in this system is the service provided by governmental agencies to the citizens (PA2). The governmental agencies retrieve guidelines for heat waves countermeasures from the block chain, where these guidelines are improved with more trustworthy through transparency and engagement. Innovative solutions are encouraged through greater stakeholder involvement engagement.

Table 5.8: Primary Assets of the QoAir case

PA #	Name	Type
PA1	Urban Heat Island measurement and detection	Information
PA2	Guidelines to heat wave countermeasures	Service

Step 2 Impact Assessment - This step determines the impact a potential compromise of a primary asset can have on seven impact areas. The primary assets have three affections, namely confidentiality, integrity, and availability. Table 5.9 shows the justification of the impact per potential compromise. The table also presents the impact score per impact area, following from Table 4.4. Here, we discuss the overall impact on each area if a compromise would occur:

Personnel: In this system, the personnel is not in any danger, and compromise of the system would not lead to any physical injuries to the personnel. Therefore, we value the overall impact on this area with an one out of five.
Capacity: Implications with the network of sensors can lead to a loss of capacity. Block chain technology ensures that the implication is reduced to a small portion of the system. The por-

tion is depending on the number of sensors in the network that are inoperable. Therefore, we value the overall impact on this area individually per compromise.
Performance: The added value of block chain technology is the decentralization of information and services. Breaches to the system could lead to quality abuse. However, this would only impact the system partially, as the rest of the block chain can remain operable. Therefore, we value the overall impact on this area between 1 (no quality abuse) and 3 (severe quality abuse that makes systems partially inoperable) out 5
Economic: The use of QoAir by governmental agencies and citizens is not purchased. Threats to the system do not result in loss of income. Therefore, we value the overall impact on this area with an one out of five.
Branding: The use, or rather misuse of information from the QoAir system by the governmental instituion would lead to complaints. Adapting wrong guidelines or wrong information sharing would raise minor concerns and local attention within the area where the system is operating in. Therefore, we value the overall impact on this area individually per compromise between one (no impact) and three (complaints and local attention).
Regulatory: The guidelines for heat wave countermeasures form take the biggest impact in this area. In case the system does not work, governmental institutions can revert to the established temperature measurements and guidelines. Therefore, we value the overall impact on this are with a two out of five, which is minor regulatory infraction.
Environment: The primary assets of QoAir's system do not affect the environment to the extent of at least short term impact, making the potential impact insignificant. Therefore, we value the overall impact on this area with an one out of five.

Table 5.9: Impact assessment of the QoAir system

PA	Compromise	Personnel	Capacity	Performance	Economic	Branding	Regulatory	Environment	Overall Impact	Justification
PA1	C	1	3	3	1	1	2	1	**3**	The measurement data is comparable to the data we now receive on weather forecasting apps. The data is open source and can be accessed by interested parties. The data that is received is not sensitive to privacy or other threats
	I	1	3	3	1	3	2	1	**3**	The accuracy of the data is crucial to the added value of the system. QoAir aims to provide more accurate measurements than current weather forecasting systems
	A	1	4	3	1	3	2	1	**4**	The availability of the data is crucial to the system to provide trigger warnings for the governmental agencies and real-time weather measurements for citizens
PA2	C	1	2	2	1	1	2	1	**2**	The guidelines are openly available. Modifications to the system should be made by a restricted selection of stakeholders
	I	1	2	3	1	3	2	1	**3**	The accuracy of the service benefits the governmental agencies constituents in providing better countermeasures against heat waves and is an important part of the system
	A	1	3	3	1	2	2	1	**3**	The availability of the guidelines is important, as the government can aid its constituents in mitigating the heat waves' effects. Even though people are able to access the information on the weather individually through the block chain, the guidelines from the governmental agency probably covers a wider range of the population

Step 3 Supporting Assets - In this step, we connect the primary assets to supporting, tangible assets. The supporting assets are the cyber components relevant to the risk assessment of the system. Table 5.10 presents the supporting assets and corresponding cyber components. Figure 5.2 shows the connections between the supporting assets and the primary assets that they affect. We present these relations in the supporting asset table with a 'x' (see Table 5.10).

The network of sensors is the first supporting asset. Even though there are several sensors, we group this into a single asset of this system. The sensors collect data which is stored in the blockchain, where the data is formed into usable data for users by the data synthesizer. The trigger generator is a control mechanism, which alerts the governmental institution in case of a heat wave in the area of the network of sensors. The last supporting asset is the distribute database in the blockchain. The database contains data from the sensors and the guidelines for heat wave countermeasures.

Step 4 Threats - We identify threats according to the supporting assets. We discuss the identified threats in this step and present them in Table 5.11. A system with hardware placed in the outside world always bears risk. From the key cyber components we find that the system of QoAir has accessible hardware for outsiders. In this case, these are the sensors in the network of weather measuring sensors. The sensors are prone to hardware failure and theft threats.

Table 5.10: Supporting Assets of the QoAir case

Cyber Components	**Supporting Assets / PAs**	PA1	PA2
Smart meters	Network of sensors	x	
Autonomous decision-making	Trigger generator	x	
Data processing/analysis tool	Data synthesizer	x	
Cloud technologies	Distributed database	x	x

(Dai et al., 2017) consider four types of security issues of blockchain within the application of Bitcoin. With Bitcoin, security issues mostly concern the financial transaction within the system. From their security issues, we find two types of threats applicable to our case. First, there is the hacking threat. Even though blockchain technology eliminates lots of security issues concerning data encryption, malicious attacks, and malware, there are still threats to the system. A form of hacking in the blockchain is the majority attack. Lin and Liao (2017) describe this as an attack by taking the majority of the computing power of a block. Although this is not as applicable to this case as it is to other fields of study, such as financial transactions, we still consider this type of attack. Another threat is a software failure. Dai et al. (2017) raise some concern on the capacity of the blockchain system to store data. Especially in the complex big data environment, the available storage space is limited.

Table 5.11: Threats for the QoAir system

Supporting Assets	**Threats**	**Primary Assets**						**Impact**
		PA1			**PA2**			
		C	I	A	C	I	A	
	Overall impact ⇒	3	3	4	2	3	3	
Network of sensors	Hardware failure			x				4
	Theft	x		x				4
Trigger generator	Hacking	x						3
	Software failure		x	x				4
Data synthesizer	Hacking	x						3
	Software failure		x	x				4
Distributed database	Hacking	x			x			3
	Software failure		x	x		x	x	4

Step 5 Likelihood Evaluation - We estimate the likelihood of risk for occurring during the lifetime of a project on a one-to-five scale. We find the estimation by taking into account what assets a person would need to attack the system, as seen in Marotta et al. (2013). We account for the time and skills the attacker need for a successful attack. Besides overall time and skill, the attacker needs specific knowledge of its target, and the target needs to be available for an attack. Table 5.12 presents the score of the threats on each of the likelihood measures and the overall likelihood scores. The most likely threat to occur is software failure, followed by hardware failure. These threats were found to be possible threats to occur more frequently than once in the project's life cycle. The failure threats can occur both with and without the intervention of humans. Therefore, software and hardware failures are likely to occur. Theft and hacking rely on the intervention of humans. Due to the benefit of blockchain technology in added security and the amount of time and knowledge, both technical and system-specific, needed for a thief or hacker, we rate these threats as remote, following Figure 4.7.

Step 6 Risk Level Evaluation - With the impact and likelihood scored in the previous steps, we can estimate the risk level. Table 5.13 presents the risk level for each threat. The level of risk determines the mitigation strategy in the next step.

Table 5.12: Likelihood of the threats for the QoAir system

Supporting Assets	Threats	Time	Knowledge	Target	Availability	Likelihood
Network of sensors	Hardware failure				x	3
	Theft	x	x	x	x	2
Trigger generator	Hacking	x	x	x		2
	Software failure				x	4
Data synthesizer	Hacking	x	x	x		2
	Software failure				x	4
Distributed database	Hacking	x	x	x		2
	Software failure				x	4

Table 5.13: Risk level evaluation of the QoAir system

Supporting Assets	Threats	Impact	Likelihood	Risk
Network of sensors	Hardware failure	4	3	**High**
	Theft	4	2	**Medium**
Trigger generator	Hacking	3	2	**Low**
	Software failure	4	4	**High**
Data synthesizer	Hacking	3	2	**Low**
	Software failure	4	4	**High**
Distributed database	Hacking	3	2	**Low**
	Software failure	4	4	**High**

Step 7 Risk Treatment - The mitigation strategies for each threat is presented in Table 5.14. With the application of blockchain technology, the pre-control of a robust network is already in place. Multiple sensors are placed in various locations, independently from each other. This distribution leads to a robust network where the failure or theft of one sensor does not affect the other sensors within the network. The same applies to the distributed database within the system. Blockchain has the benefit of storing the information in each users' block, making the system robust by not relying on a central database. With the identified threats, we seek to control in case of (software) failure. A backup protocol should protect the system in case a threat occurs. The use of such a protocol gives each stakeholder the responsibility to act according to the protocol.

Table 5.14: Risk treatment for the QoAir system

Supporting Assets	Threats	Mitigation Strategy	Pre-controls	Post-controls
Network of sensors	Hardware failure	Indemnification	Robust network	backup protocol
	Theft	Mitigation		backup protocol
Trigger generator	Software failure	Indemnification	Robust network	backup protocol
Data synthesizer	Software failure	Indemnification	Robust network	backup protocol
Distributed database	Software failure	Indemnification	Robust network	backup protocol

5.3 CROSS-CASE SYNTHESIS

5.3.1 High-risk threats

From both risk assessments, we find numerous threats to the system. In this section, we summarize the high-risk threats and mitigation strategies of both assessments and discuss the findings. We identify similarities and differences to report the main takeaways from the case study in terms of risks to innovation projects in climate disaster resilience.

For the assets in the GM4W system, we find several types of high-risk attack threats. GNSS satellites and receivers are prone to two types of attacks, namely signal jamming and signal spoofing. Data stored on hardware is vulnerable to data loss due to factors such as hardware failure and theft of the hardware. Data on the cloud faces numerous threats, of which the denial of cloud services carries a high risk to the system. The power source, either solar power or the conventional electrical grid, can be a threat when unable to provide power to the system. Within the system, we have specialized staff and customer help service staff. Both of these staff members are prone to human error and insider attack threats. From the key cyber components, we find that the system of QoAir has accessible hardware for outsiders. In this case, these are the sensors in the network of weather measuring sensors. The sensors are prone to hardware failure and theft threats. Even though blockchain technology eliminates lots of security issues concerning data encryption, malicious attacks, and malware, there are still threats to the system. We find the capacity of the blockchain system to store data as software failure threat that bears a high risk.

The two systems show some similarities. Both systems have weather-related measuring infrastructures to provide information efficiently. The main difference is the distribution and storage of information. GM4W has centralized data storage, whereas QoAir uses the decentralized distribution of information through blockchain technology. The blockchain technology eliminates many software-related threats with encrypted data transfers and distributed data storage. However, we still find software failure as a high risk. The hardware-related threats of the two systems are similar. Accessible hardware components are prone to theft, and hardware may fail. A difference in the systems comes with the staff members in the GM4W system. The specialized staff and customer helpdesk service staff have access to the system and are prone to human errors and insider attacks. The human involvement in the QoAir is limited to each users' block, taking away the human-related threats as high risk. The comparison of risks exposed to categories of risks. We find risks related to software, hardware, and humans (see Figure 5.3).

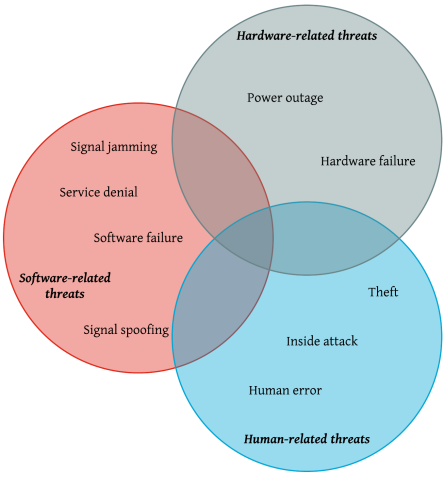


Figure 5.3: The identified threat categories from the risk assessments

5.3.2 Risk treatment

Signal jamming (including service denial) and spoofing are high-risk threats on the transmission of data. The countermeasures involve integrity monitoring and detection of signals, encrypting the data, and the prioritization of critical receivers. For the cloud and local storage, we found similar countermeasures of data encryption and backup protocols for both the local storages and cloud environments. Building a robust network ensures the continuation of the process in case of incidents. Setting up a backup protocol to ensure the continuation of the processes may the threats occur. Timely backup is the primary mitigation strategy. The backups should follow a periodical protocol with everyone involved strictly following it. The dependency of power to this system complicates the mitigation of this threat. Using backup generators is a way to ensure the system's continuation. A way to address the limited capacity of generators is to prioritize critical assets.

The QoAir assessment provides blockchain threat mitigation strategies with a robust network and backup protocols. We mentioned these controls in the GM4W assessment, and see these controls as general good practices for risk treatment. Data encryption and integrity monitoring are controls for software-related threats more specific to the GM4W. However, QoAir does not have these threats because of the blockchain technology that it uses. This technology internally encrypts data and monitors data transmissions.

Human threats involve theft, insider attacks, and human errors from staff members. The first mitigation step here is identity and access. The system should monitor who accesses what information and whether this person is allowed to do so. Training the staff mitigates human errors to some extent, using a backup to create a robust system in case of incidents also can achieve this mitigation.

5.4 CHAPTER CONCLUSION

This chapter presented the risk assessments of the case studies. First, we subjected the GM4W system to a risk assessment. The system's main data transmission was GNSS data. High-risk threats were jamming and spoofing of signals, failure of hardware, theft, insider attack, human errors, and power outage. Some of these threats have similar mitigation measures. The most important measures are data encryption, a backup protocol, creating a robust network, prioritize critical assets, and integrity monitoring. Second, we had a risk assessment of QoAir. The system's main data transmission here was sensor data through a blockchain infrastructure. Theft or failure of hardware components is a high-risk to this system, along with software failure. We found two of risk treatment controls in this assessment with a robust network and backup protocols.

The cross-case synthesis compared the threats to both systems, and we distinguished three types of threats from this comparison, namely hardware-related, software-related, and human-related threats. We compared the risk treatment controls as well. Creating a robust network and having backup protocols are controls identified in both assessments and general good practices for risk treatment. Data encryption, integrity monitoring, staff training, and identity and access control are controls for software- and human-related threats more specific to the GM4W.

The next chapter will use the results from this chapter to design the extension of the TIF. After that, we conclude this study with the conclusion in Chapter 7.

6 EXTENSION OF THE TIF

This chapter will answer the fourth sub-question in this research: Where can cyber risk management be of importance in the Test and Implementation Framework (TIF) of BRIGAID? Section 3.1.1 briefly introduces the TIF, which we address in greater detail here. After the introduction of the framework, we identify potential slots within the framework where we can implement a cybersecurity extension. Next is the design of the cybersecurity extension (Section 6.2). Note that this design uses results from both Section 2.3 and Chapter 5. Section 6.3 continues with a reflection on the design and implementation guidelines, and we validate the tool in Section 6.4. Section 6.5 concludes the chapter.

6.1 CURRENT TIF TOOL

This section will introduce the TIF in greater detail than is done before (see Section 3.1.1). Sebastian et al. (2019a) is the final version of the guide that is in support of the TIF tool. The guide elaborates on the explanation of the tool and the mechanisms behind the assessment scoring system. In this section, we follow the structure of the guide. We analyze climate adaptation innovation projects as socio-technical systems in the TIF. From this type of system, we derive three assessments, namely technical testing, impact assessment, and social testing (Sebastian et al., 2019a).

6.1.1 Technical Testing

The technical characteristics of the projects are assessed based on their technology readiness level (TRL). The TRL measurement in support of the technical maturity assessment of technological projects. The measurement originates from the technology planning of NASA space technology (Mankins, 2009). The scale is adopted in the TIF tool and modified to fit the needs of climate adaptation innovation. Despite the well-accepted status, the TRL measurements do have limitations concerning the assumed linearity of technological development and the framing on technical maturity instead of technical readiness (Sebastian et al., 2019a). BRIGAID addresses these concerns by forming the TRL in a scale consisting of four so-called stage gates. These stage gates are soft borders of certain milestones in the development process. An assessment accompanies each stage-gate, and innovators are advised to revise the previous phase if the assessment results in major concerns. The border is soft in the sense that innovators are free to choose whether to assess their progress and how to interpret the results of a performend assessment.

The technical readiness of an innovation project is measured based on four performance indicators in the TIF tool assessment (see Table 6.1). The technical effectiveness of an innovation project tests the functionality of the innovation in terms of risk reduction. The durability determines the lifetime of a project and the operational activity during that lifetime. A system can have three statuses, namely active, inactive, or stand-by. Stand-by status for innovation projects are permanently implemented systems that operate when a hazard occurs. The third technical performance indicator is the system's reliability. The reliability of a system is the inverse of the failure probability, i.e. the reliability is 100% minus the probability of a system failure. The final performance indicator is the flexibility of a system. The goal of BRIGAID is to, eventually, serve as a global quality label for innovation in climate adaptation (see Sec-

tion 1.1.2). The flexibility measures whether we can implement a system in other locations, without complications to the system and high costs.

Table 6.1: Performance indicators, derived from Sebastian et al. (2019a)

Assessment	Performance Indicators	
Technical	Technical effectiveness	Reliability
	Durability	Flexibility
Impacts	Sustainable design	Forestry
	Environmental impact	Health
	Ecological impact	Infrastructure
	Agriculture	Tourism
	Energy	
Societal	Psychometric risk factors	User acceptance constructs
	Inflexibility indicators	Responsibility dimensions
	Sociocultural preferences	

Table 6.2: System status options for types of system durability, types adapted from Sebastian et al. (2019a)

Durability	Operating status
Permanent	Active
Semi-permanent	Active, stand-by
Temporary	Active, inactive
Continuous operation	Active
Operation prior to/during a hazard event	Active, stand-by

6.1.2 Impact Assessment

Climate adaptation innovations will have a certain impact on the environment. The projects are designed to tackle one of several climate disasters. The effect is often direct, for example, with an innovation project on flood protection, where the protection directly affects the river or sea it is built-in. Besides these, often intended, direct effects, projects also have indirect effects on the environment. These can be both positive and negative effects. When assessing the ecosystem, we identify lots of cause and effect relations, some that are still unknown (Loreau et al., 2001). This uncertainty results in surprising or even undesired indirect effects from adaptation projects. To account for these events, the TIF uses an impact assessment. This impact assessment scores the project based on three performance indicators, namely sustainable design, and the environmental and ecological impacts. The environment in itself has several socio-economical sectors that can be affected, both positively and negatively, by a climate adaptation innovation. BRIGAID focuses on six socio-economic sectors when assessing the innovation's environment, namely agriculture, energy, forestry, health, infrastructure, and tourism.

Figure 6.1 shows the system of climate disasters and the effects adaptation and innovation projects have on the occurrence and impact of climate disasters. Arrows represent the effects from one element to the affected element. A positive relation is illustrated with a plus sign, whereas a minus sign represents a negative relation. For example, climate adaptation and innovations have a positive effect on climate change mitigation, meaning more innovations result in more mitigation effects. The negative relation of adaptation is good in the sense that more adaption and innovation leads to less impact of climate disasters. The relation of adaptation and innovation in the environment does not weigh positively or negatively. The relation can be either negative or positive and depends on the effects resulting from the adaptation or innovation. Each of the socio-economic sectors serves as a performance indicator in the impact assessment of the TIF tool.

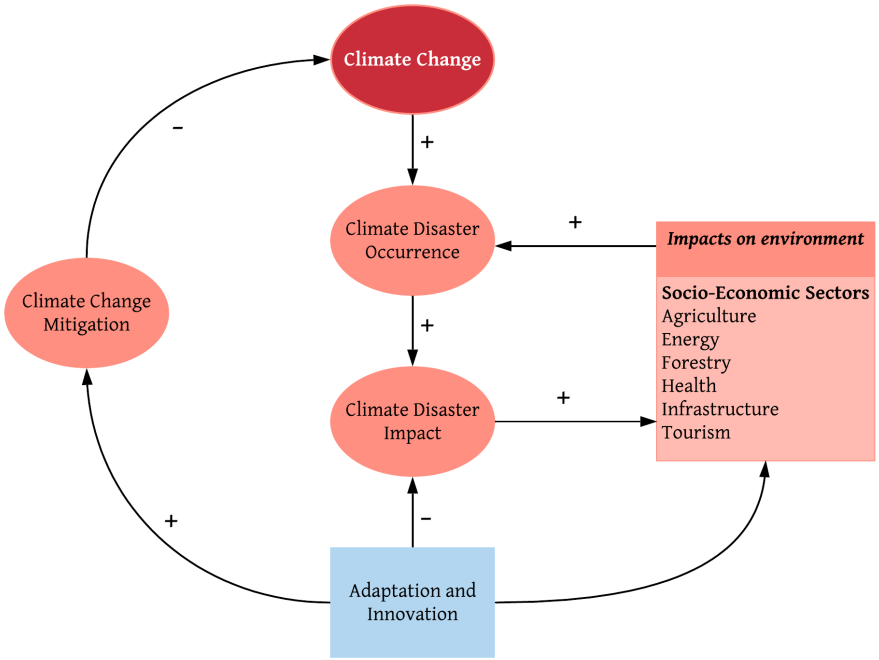


Figure 6.1: System diagram of climate disaster adaptation, own image derived from Sebastian et al. (2019a)

6.1.3 Social Testing

The final part of the TIF assessment tool addresses the societal concerns that innovations might raise. Sebastian et al. (2019a) derives five performance indicators from the literature review to structure the assessment on societal acceptance. The first indicator concerns psychometric risk factors. These are factors on how end-users and society perceive innovations. Inflexibility indicators is a second indicator. This indicator focuses on the organization of innovations and the management of technology. Thirdly, we have socio-cultural preferences. This indicator is important in the context of Europe. The wide variety of cultures and social constructs in Europe ask for different implementation methods. Innovations are scoring high on this indicator if the implementation doesn't carry high costs and risks. Since this is often not the case with climate adaptation innovations, responsibilities for implementation, financing, and risk-bearing must be addressed before offering the innovation on the market. Fourth, we have user acceptance constructs. This indicator isn't necessarily on the performance of the innovation, as it is more on the perception of users on the innovation's performance. The innovation should bring benefits to the user, either by being easy to operate or meets the subjective standards of users. The final indicator of social acceptance addresses the responsibility dimension. Responsibility, in this case, concerns the responsible practice of research, development, and performance. We assess innovators on the different uses of their projects, the robustness of the innovation's performance, and involving all stakeholders.

6.2 EXTENSION DESIGN

With the current structure of the TIF tool as a base, we continue with the design of a cybersecurity extension. First, we focus on potential space where to place a cybersecurity extension. The current tool operates in Microsoft Excel. Excel is a spreadsheet tool that can store, analyze, and visualize data in one file. Innovators can answer the questions in the different sheets per category. Excel calculates the score based on the answers of the innovators and BRIGAIDs formulas. A separate sheet is created to present a summary of the scores and visualize the results with a score table and graphs (see Figure 6.2). The sheets of different categories work independent, i.e. each category can be assessed individually. With creating the extension, we must choose between extending one of the categories (Figure 6.3) and creating a new sheet for

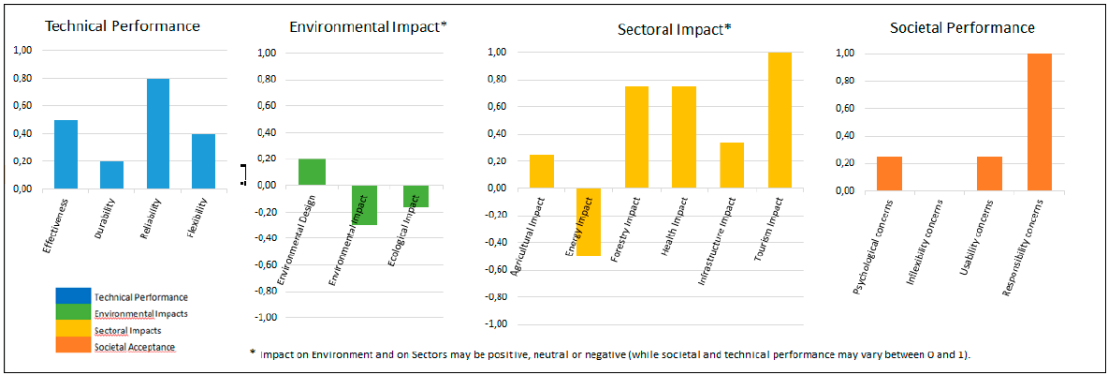
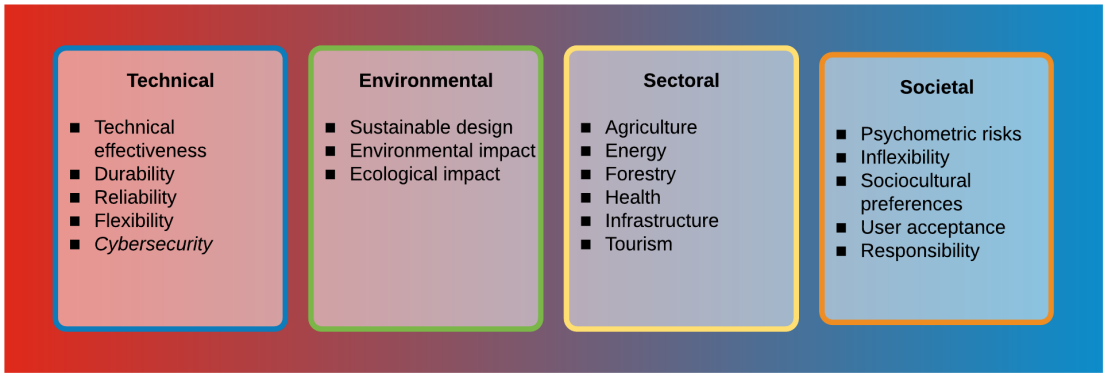


Figure 6.2: Example of TIF output for an innovation (Rica et al., 2017)

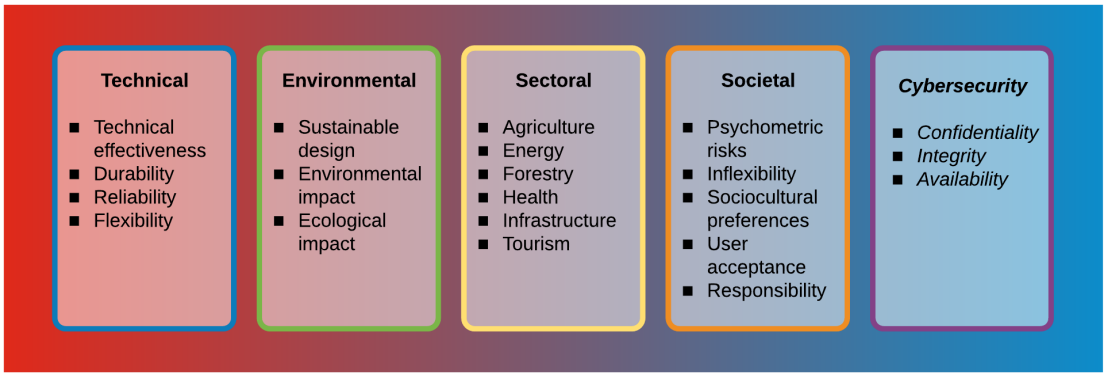
cybersecurity (Figure 6.4). Designing a new sheet as a standalone assessment would maintain the structure of the tool. We consider the potential addition to one of the existing categories as well. Adding cybersecurity to an existing category means that cybersecurity must have significant overlap with the category's current performance indicators or that cybersecurity questions benefit the robustness of current indicators. The addition will make sense if we add a limited set of questions to the tool. The addition of too many questions impacts the assessment's impact in terms of user fatigue and ease of operating. It also changes the category's process and scoring system, and the validation of the assessment as a whole needs a re-examination. Results show that the cybersecurity assessment for systems is standardizable to some degree, but this needs a certain number of questions that will complicate the category assessment as a whole. Current assessment questions consider the safety of the system. The assessment tool already addresses the technical, environmental, and societal concerns on safety. The impact of innovations on sectors also takes safety into account. However, the security of the system itself is out of the scope of the current tool. Therefore, we choose to design a separate sheet for cybersecurity, making it a new category in the TIF tool. Despite the usability of questions in other categories, we assess cybersecurity separated from the other categories. This independency makes our extension a standalone assessment tool within the TIF for the security of information and services as provided by innovations. Innovators may choose to solely assess the cybersecurity of their system at any point of development without the need to assess their innovation in all categories. We continue with the design of the new assessment for the cybersecurity of innovations.



The first extension option is to add cybersecurity as a Performance Indicator to the Technical Readiness assessment of the TIF tool. A scoring mechanism for cybersecurity and extra questions are added, and current technical readiness question can be utilized as well

Figure 6.3: First option for the TIF extension design

There are numerous ways to assess the cybersecurity of a system. Section 4.3 shows the variety of methodologies and how we chose to follow the SecRAM method for the risk assessments



The second extension option is to create a new assessment category to the TIF tool. Cybersecurity will have questions in three categories, resulting in scores on three new Performance Indicators: Confidentiality, Integrity, and Availability

Figure 6.4: Second option for the TIF extension design

of this study. The CIA characteristics of assets are briefly discussed in Section 4.3.4. The characteristics, confidentiality, integrity, and availability of assets are the main focus in the SecRAM risk assessment. We assess the assets of systems based on the presence of these characteristics. There are various ways to structure the cybersecurity assessment. The TIF tool asks for a simple structure, similar to the structures of the assessments in place currently. The other categories either use yes or no questions or multiple choice questions with three answer choices (A, B, or C). We similarly structure the new cybersecurity assessment and use yes or no questions. The yes and no answering options create an accessible and straightforward assessment and make room for more items, covering a more comprehensive range of possible subject for the questions. We divide the assessment into three subcategories, each covering one of the CIA characteristics. In this design, each of the three CIA characteristics represents a Performance Index for cybersecurity (see Figure 6.4). We now present the performance indices.

Confidentiality
The confidentiality of assets determines how information and services are disclosed to its users. Confidentiality is breached when unauthorized entities gain access to the asset.

Integrity
The integrity of an asset determines whether the asset provides information and services as it was intended. The asset should provide the full information and services without outsider's breach of that information.

Availability
The availability of information and services should be available whenever an end-user needs it, without interference or obstruction.

With the structure of the extension set, we continue with the content of the assessment tool. These are the questions that innovators answer to self-assess the cybersecurity readiness of their innovation project. We divide the questions in the cybersecurity assessment into four sections, namely service, data transmission, hardware, and identity and access. Each of these sections contains questions that affect high-risk threats to innovation projects found in the risk assessments in Chapter 5. Figure 6.5 shows which sections cover what performance indicators of cybersecurity.

Firstly, the service section covers the electricity dependence of the project (see Table 6.3). The questions determine whether the project needs electricity and if so, what protocol is in place in case of a power outage, which is identified as a high-risk threat. An innovation that remains in operation during a power outage, either by operating offline, prioritizing critical assets in

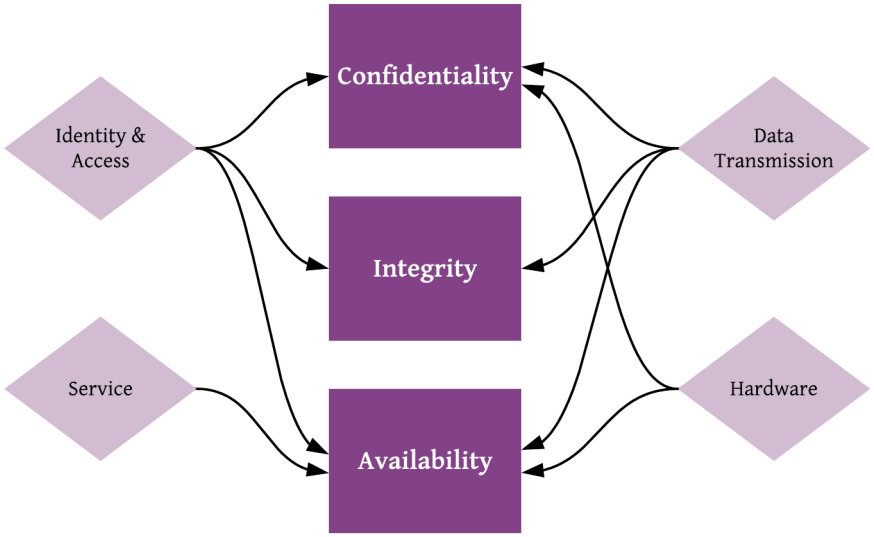


Figure 6.5: Causality of the questions on the performance indicators

case of limited supply or a backup protocol, is prepared for this threat. This threat influences the availability characteristic of the system's cybersecurity.

Table 6.3: Assessment questions in the Service section

1	Service	C	I	A
1.1	Does any part of your innovation's system require electricity?			✓
1.2	Is there a protocol in place in case of power outage or other disruption of service?			✓
1.3	Does your innovation have a protocol in case of limited power supply?			✓
1.4	Is the innovation able to operate without an internet connection?			✓

Secondly, we have the data transmission, which is found to be the primary process in the system from a technical perspective (Information Security Officer, ABN Amro, 2019). Table 6.4 presents the questions in this section of the cybersecurity assessment. There are a total of nine questions in this section, influencing all three performance indicators. The section has two parts, one covers the high-risk threats for the communication of data, while the other part covers data storage threats. Data communication threats involve signal jamming and spoofing, hacking, and malware. Questions in this part assess the communicating components in the technical perspective. These are questions involving servers, firewalls, and mitigation strategies such as backup protocols and data encryption. Items in the data storage part include questions about the system's storage facilities and its security. We also assess the privacy concerns of data. Threats covered in this part are human errors, insider attacks, and theft.

Thirdly, we assess the hardware of a system (see Table 6.5). The location and security of the system's devices are subject to the questions in this section. Theft, hardware failure, insider attacks, and signal jamming and spoofing are threats we consider in this section for the confidentiality and availability of the system.

Lastly, we have the identity and access section, as presented in Table 6.6. This section covers all three performance indicators and mainly focuses on human errors and insider attack threats. We ask the innovator about the accessibility of the system, both for authorized and unauthorized entities. We ask questions on the freedom people have when entering and working in the system, and whether this is controlled. The aim is to find out how prepared the system is against human errors and threats from the environment. Suppliers are essential stakeholders

Table 6.4: Assessment questions in the Data Transmission section

2	Data Transmission	C	I	A
2.1	Does any part of your innovation's system require the transmission of data?	✓	✓	✓
2.2	Does your innovation have servers sending or receiving data?	✓	✓	✓
2.3	Does your innovation have firewalls for the protection of your servers?	✓	✓	✓
2.4	Does your innovation store data?	✓	✓	✓
2.5	Is stored data in the innovation's system protected from unauthorized access?	✓		
2.6	Does the data used by the innovation contain sensitive data (privacy, legal, ethical)?	✓	✓	
2.7	Is data transmission within your innovation secured?	✓		
2.8	Is the validity of the data in your innovation regularly monitored?		✓	
2.9	Is there a backup protocol in case of loss of data?		✓	✓

Table 6.5: Assessment questions in the Hardware section

3	Hardware	C	I	A
3.1	Does any part of your innovation's system require hardware?	✓		✓
3.2	Is any hardware belonging to your innovation placed in an on-site location?	✓		✓
3.3	Is the site location of your innovation secured?	✓		✓
3.4	Is any hardware belonging to your innovation placed out in the open?	✓		✓
3.5	Are the hardware elements of the system protected against outsiders?	✓		✓

in a system. The cybersecurity of the system also depends on the security efforts made by suppliers of assets and components that are used in the system. This section assesses the threat of vendor lock-in. Vendor lock-in is the event in which all of the external parts of a system come from one vendor. This situation creates a significant dependency on that one vendor, who can exploit this dependency by excluding competition from offering their services to the innovator (Information Security Officer, ABN Amro, 2019).

Table 6.6: Assessment questions in the Identity & Access section

4	Identity & Access	C	I	A
4.1	Does any part of your innovation's system require access for staff members?	✓	✓	✓
4.2	Does your innovation have control for identification of accessing entities?	✓		✓
4.3	Does your innovation have a clear distinction in the authorization of different entities?	✓		
4.4	Is the data within your innovation openly accessible to the ones in need of that data?	✓		✓
4.5	Do users have access to the innovation at all times?			✓
4.6	Are entities with access to the innovation's system trained to limit human errors?	✓	✓	
4.7	Does any part of your innovation's system require outside parties' access?	✓		
4.8	Is every part of your innovator's system built within your own company?	✓		

6.3 EXTENSION IMPLEMENTATION

Within the implementation part of the tool extension, we see how the extension is implemented in the current tool. The TIF is designed in Microsoft Excel. Each assessment has its sheet in the Excel file with a link to the summarizing sheet that shows the results of the entire assessment. We need to implement the cybersecurity extension in a new sheet. We pose the questions and model the scoring system according to the design of the current tool to align the extension to the rest of the TIF tool. Figure 6.6 presents the questions in the cybersecurity extension of the tool as captioned in the Excel file. We formulate the scoring system in the same form as the scoring systems of the other assessments (see Algorithm 6.1). The pseudo code shows the formulas for the three performance indicators. The results are presented in the form of the following sentences:

- Your innovation raises [C] concerns related to confidentiality, having scored [X1] out of a possible [Y1] and is [Z1] from/to being ready/effective in terms of its cybersecurity.
- Your innovation raises [I] concerns related to integrity, having scored [X2] out of a possible [Y2] and is [Z2] from/to being ready/effective in terms of its cybersecurity.
- Your innovation raises [A] concerns related to availability, having scored [X3] out of a possible [Y3] and is [Z3] from/to being ready/effective in terms of its cybersecurity.

The variables in between brackets are the formulas we present in Algorithm 6.1. The question that apply to a performance indicator are counted in the Y variable. Only questioned that are filled in with an answer are considered for the score. The answer determines if a project scores positive (1) or negative (0) on the indicator. The scores are counted in the X variable.

1 Service
1,1 Does any part of your innovation's system require electricity?
1,2 Is there a protocol in place in case of a power outage or other disruption of service?
1,3 Does your innovation have a protocol in case of a limited power supply?
1,4 Is the innovation able to operate without an internet connection?
2 Data Transmission
2,1 Does any part of your innovation's system require the transmission of data?
2,2 Does your innovation have servers sending or receiving data?
2,3 Does your innovation have firewalls for the protection of your servers?
2,4 Does your innovation store data?
2,5 Is stored data in the innovation's system protected from unauthorized access?
2,6 Does the data used by the innovation contain sensitive data (privacy, legal, ethical)?
2,7 Is data transmission within your innovation secured?
2,8 Is the validity of the data in your innovation regularly monitored?
2,9 Is there a backup protocol in case of loss of data?
3 Hardware
3,1 Does any part of your innovation's system require hardware?
3,2 Is any hardware belonging to your innovation placed in an on-site location?
3,3 Is the site location of your innovation secured?
3,4 Is any hardware belonging to your innovation placed out in the open?
3,5 Are the hardware elements of the system protected against outsiders?
4 Identity & Access
4,1 Does any part of your innovation's system require access for staff members?
4,2 Does your innovation have control for identification of accessing entities?
4,3 Does your innovation have a clear distinction in the authorization of different entities?
4,4 Is the data within your innovation openly accessible to the ones in need of that data?
4,5 Do users have access to the innovation at all times?
4,6 Are entities with access to the innovation's system trained to limit human errors?
4,7 Does any part of your innovation's system require outside parties' access?
4,8 Is every part of your innovator's system built within your own company?

Figure 6.6: ScreenScreensScreeScreenScreenshotof the cybersecurity extension in the TIF tool

Algorithm 6.1: Pseudo code of the formulas in the cybersecurity extension

```
C = if X1 / Y1 ≤ 0.4 then
    "many" [concerns]
else
    "some"
end
I = if X2 / Y2 ≤ 0.4 then
    "many" [concerns]
else
    "some"
end
A = if X3 / Y3 ≤ 0.4 then
    "many" [concerns]
else
    "some"
end
X1 = Count the cells with "Yes" for Questions 2.3, 2.5, 2.7, 3.3, 3.5, 4.2-4.3, 4.6, 4.8 + count the cells
     with "No" for Questions 2.1-2.2, 2.6, 3.1-3.2, 3.4, 4.1, 4.4, 4.7
X2 = Count the cells with "Yes" for Questions 2.3, 2.8-2.9, 4.6 + count the cells with "No" for Questions
     2.1-2.2, 2.4, 2.6, 4.1
X3 = Count the cells with "Yes" for Questions 1.2-1.4, 2.3, 2.9, 3.3, 3.5, 4.2 + count the cells with "No"
     for Questions 1.1, 2.1-2.2, 2.4, 3.1-3.2, 3.4, 4.1, 4.4-4.5,
Y1 = Count the number of answered questions for Questions 2.1-2.7, 3.1, 3.5, 4.1-4.4, 4.6-4.8
Y2 = Count the number of answered questions for Questions 2.1-2.4, 2.6, 2.8, 2.9, 4.1, 4.6
Y3 = Count the number of answered questions for Questions 1.1-1.4, 2.1, 2.4, 2.9, 3.1-3.5, 4.1-4.2, 4.4-4.5
Z1 = if X1 / Y1 ≥ 0.5 then
    "close" [to being ready]
else
    "far"
end
Z2 = if X2 / Y2 ≥ 0.5 then
    "close" [to being ready]
else
    "far"
end
Z3 = if X3 / Y3 ≥ 0.5 then
    "close" [to being ready]
else
    "far"
end

```

6.4 TOOL VALIDATION

For the validation of the tool, we use the Technology Acceptance Model (TAM) (see Figure 6.7). The TAM as a method aims to model the acceptance and intention of users to use a new technology (Davis et al., 1989). For this case, we interview the Project Manager of BRIGAID to model his intention to use and general attitude towards the extension. The interview, conducted on 10 September 2019, was semi-structured around the following questions:

1. Does the risk assessment benefit the TIF? (U)
2. Does the risk assessment result in new insights with respect to innovation project assessment? (U)
3. Are there any improvements you see when assessing the tool extension? (U)
4. Do you believe the risk assessment to be an improvement of the current tool? (E)
5. What are barriers to adopting this extension of the tool do you see, if any? (E)

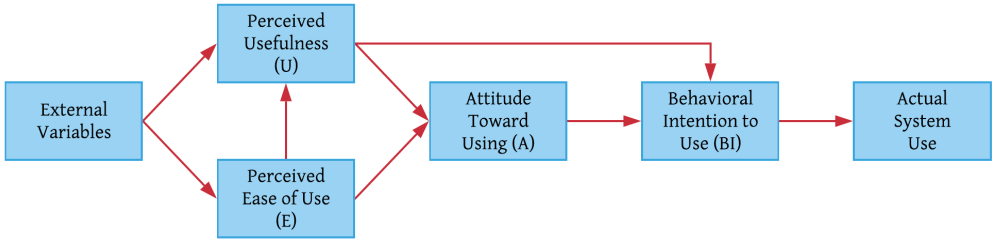


Figure 6.7: Technology Acceptance Model. Adapted from Davis et al. (1989, p.985)

We designed the questions to answer a block in the model, as presented in Figure 6.7. The letter of the block that the question addresses is reported in between brackets. The semi-structured interview gave us an openness to elaborate on certain questions to model the perceptions and intentions according to the model.

Figure 6.8 presents the model with the results of the interview. The results show that the perception towards the extension is positive. We determined a positive attitude towards the extension and the intention to use. The main drawback and barrier is the intention of the BRIGAID partners and innovators. The model should be applied to these stakeholders as well, to determine their intention to use as well. We find that the Project Manager of BRIGAID intends to propose the extension to the experts and partners of the program. A positive attitude toward using from these stakeholders leads to an intention to use and ultimately to the actual use of the system.

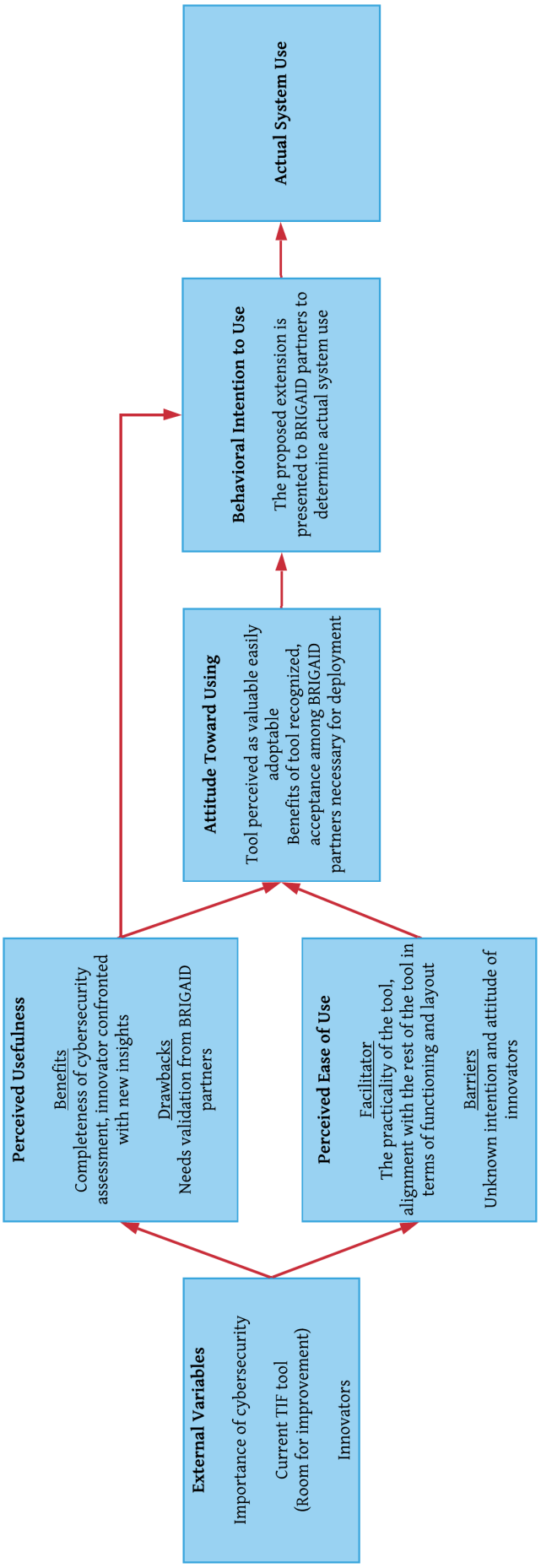


Figure 6.8: Technology Acceptance Model for the cybersecurity extension of the TIF

6.5 CHAPTER CONCLUSION

This chapter aimed to answer the fourth sub-question of this research: *Where can cyber risk management be of importance in the TIF of BRIGAID?*. First, we discussed the current TIF. Three assessment groups were identified, divided into the four categories of the current tool. The structure of the different assessments is similar in the sense that we ask mere clear questions and score them according to manageable equations. There are two types of questions, namely yes/no and multiple-choice questions. The assessments have performance indicators to indicate where the project potentially is lacking.

From the current tool, we identified two types of extensions. One is to add cybersecurity as a performance indicator to the technical testing of the tool. The other is to create a separate assessment category for cybersecurity, with its performance indicators. We chose the latter for the design of the extension. The standalone assessment tool for cybersecurity is expected to provide a more extensive assessment of the system. The CIA characteristics are the assessment's performance indicators, and questions that influence these type of threats are influencing their score. The assessment tool asks the innovators four types of questions, namely service, data transmission, hardware, and identity and access. To validate the tool, we used the Technology Acceptance Model to find the usefulness and ease of use of the tool, as perceived by the Project Manager of BRIGAID. We found that the Project Manager perceives the tool as useful and that there is an intention to use the tool. However, the partners and innovators of BRIGAID need to have the same perception of usefulness and intention to use for the extension to be implemented.

The next chapter concludes this thesis. The research questions are presented once again and answered according to the findings of this study. We present recommendations for the use and possible improvements to the extension of the TIF.

7 CONCLUSION

This chapter concludes the thesis. The main research question is revisited and answered in a stepwise approach by answering the sub-questions in Section 7.1. After presenting the main conclusions, we continue with a critical reflection by summarizing the research and placing our findings in the intended context of innovation, both in climate disaster resilience and beyond (Section 7.2). We discuss the limitations of this study. The relevance to policymakers, innovators, and the scientific field are discussed, as well as the alignment with the Engineering and Policy Analysis Master's curriculum. Finally, we leave the reader with the contributions of this study and recommendations for innovators and academic research (Section 7.3).

7.1 CONCLUSIONS

The objective of this study is to assess the relevancy of cybersecurity in BRIGAIDs Test and Implementation Framework (TIF) and to develop an extension to the TIF in which cybersecurity threats can be identified and mitigated effectively. We focus specifically on innovations for climate disaster resilience, as featured in the BRIGAID program. We posed the following main research question:

How can cybersecurity threats be effectively identified and mitigated to minimize the risk of cyber attacks on innovation projects for climate disaster resilience?

To answer this question, we posed five sub research questions, each aimed at one part of the research. Here, we will present each sub-question with the findings on the question from this study. These conclusions lead us to the main conclusion of this study, where we answer the main research question.

What type of cyber components can be distinguished when assessing risks in innovation projects?
The answer to this question follows from the literature review, expert interviews, and the results from the survey in Chapter 2. We first assessed related fields of study, such as the Internet of Things, SCADA, and smart technologies. From the results, we formed a framework with four elements of innovation projects. The freedom of innovation was found to be essential and unique to innovation. The freedom to work in a system and improve it is a crucial trade-off with the security of that system. The human factor and human interactions merged in the roles and responsibilities element. The cyber part of innovation is covered by the information architecture element, while the physical security element houses the physical side of the system.

Within those last two elements, we identified the space for cyber components. Cyber components are parts of the cyber-physical system of innovation projects, and we categorized them into five elements, namely components of data collection, communication, data processing, and control, and physical components. Through expert validation data, we found the categorization to be subjective and not leading when assessing key cyber components. After the survey data, we compiled a list with key cyber components, with components in differing categories from the initial list (see Figure 7.1). The data from the interviews also showed the different perspectives in which we assess the cybersecurity of systems. We initially used a physical perspective when assessing the cyber components. Following the SecRAM method-

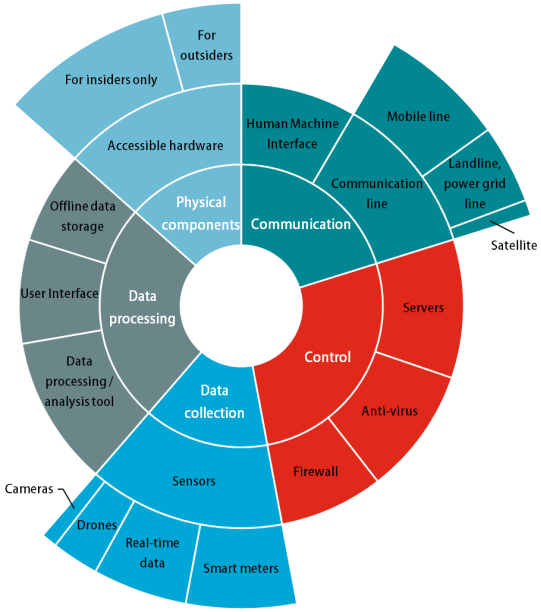


Figure 7.1: The identified key cyber components

ology, we changed to a technical perspective, focusing more on the functioning components and assessing these according to the confidentiality, integrity, and availability categorization.

What innovation projects within the BRIGAID project can provide the broadest variety of cyber components?
The answer to this question follows from Chapter 3. We used the identified key cyber components and the data from BRIGAID to identify two representative cases. From the survey data, we divided the innovation projects based on the perceived importance of cybersecurity and satisfaction with current cybersecurity efforts. We sought a project with high perceived importance for cybersecurity, and one with much satisfaction with ongoing efforts. Systems of potential cases should include the majority of the key cyber components and address different climate disasters. We found GM4W as a much-satisfied project with current cybersecurity efforts, while we found QoAir as the project with a high perceived importance of cybersecurity. GM4W covered nine of the key cyber components. This project uses GNSS sensors to predict heavy precipitation on a local scale. The system uses a centralized data distribution and storage concept. QoAir covered ten of the key cyber components. The project of QoAir uses blockchain technology to measure urban heat islands more effectively than current weather measuring sensors. The transmission of data through blockchain provides a decentralized distribution. The differences in the structure of the systems provide us with a wide variety of components and processes.

What type of cyber risk assessment methods are applicable to risk assessment of innovation projects?
The answer to this question follows from Chapter 4. We performed a literature review to find a suitable method for this research. The search is performed across the field of innovation and recent technology, similarly to the analysis in which we compiled the list of cyber components. Other fields of study, such as IoT, SCADA, and smart technology, showed more available methods. We established three selection criteria to narrow down the list of methods for risk assessment. First, we chose between quantitative and qualitative assessment methods. Qualitative methods use a subjective classification of the level of risk in a system. Quantitative methods measure risks with numerical data and often are probabilistic of nature. While the objective data of quantitative methods is preferred, the downside of these methods is the need for empirical data. We conclude that in the case of innovation projects with limited data avail-

able, we qualitatively assess the risks. The second criterion is the classification of assessment methods from Cherdantseva et al. (2016). The need for a complete risk assessment, including all steps, and the lack of need for a high level of detail leads us to guideline methodologies. The last criterion is the applicability of the method. A feature of this research is the projects subject to it. The wide variety of projects we could use in the assessment made it necessary for the method to apply to different project's needs.

The literature review and selection based on the criteria led us to the SecRAM methodology. The methodology uses the ISO 27005 standard for information security risk management as a base. The method is used in different fields of study and was deemed as applicable to a variety of cases, while still delivering a complete assessment of the innovation system's risks. We categorized the risks according to the CIA principles (confidentiality, integrity, and availability), and the assessment applies to the wide variety of systems that we found when assessing innovations. The qualitative, stepwise approach leads us from context establishment to risk management strategies.

Where can cyber risk management be of importance in the TIF of BRIGAID?
The answer to this question follows from Chapter 5 and Chapter 6. The results of the survey showed a difference in the impact of risks and the innovators' perception of the importance of cybersecurity. Within the TIF , we found two options for a cybersecurity extension. First, we had the option to add a cybersecurity performance indicator to the technical readiness assessment of the tool. Questions already available in this section are usable to the scoring system of cybersecurity without affecting the autonomy of the technical testing section. This option, however, would impact the size of the section and limit the cybersecurity assessment to a single performance indicator. The second option is a new assessment section for cybersecurity. By designing the new sheet as a standalone assessment, we maintain the structure of the tool. The cybersecurity can be designed in more detail and be assessed according to several performance indicators, leading to a more detailed assessment and advice.

We found the option of a new section for cybersecurity to be the preferred option. We designed the cybersecurity assessment in more detail, and we based the cybersecurity score on three performance indicators, namely confidentiality, integrity, and availability. Each of the indicators is scored based on a set of questions specifically aimed at the indicator. The main takeaway of this sub-question is that we validated the perceived usefulness of the extension with an application of the Technology Acceptance Model by interviewing the Project Manager of BRIGAID. He found the extension to be a thorough assessment which confronts innovators to new insights of their system. We conclude that the tool aligns with the rest of the TIF. However, we need the perception and intention of the partners of BRIGAID to be positive as well for the implementation of the cybersecurity extension.

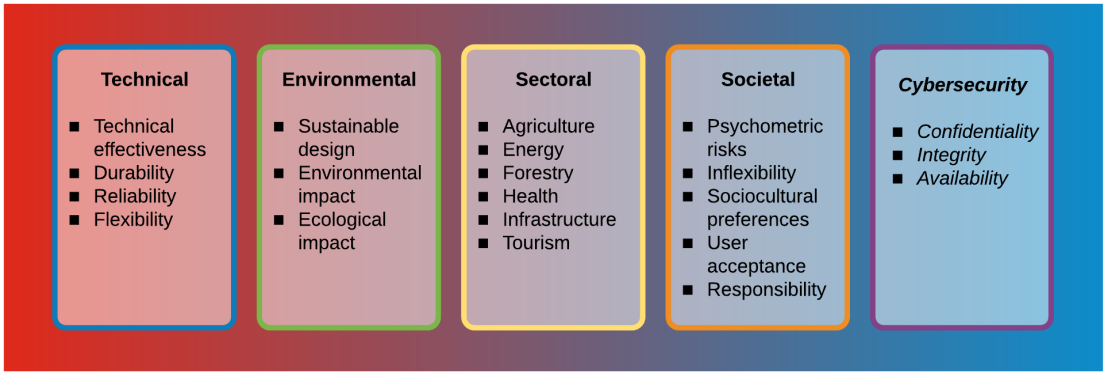


Figure 7.2: The proposed cybersecurity extension of BRIGAIDs TIF tool

What recommendations can be made based on the risk assessment of innovation projects for climate disaster resilience?
The answer to this question follows from Chapter 5. The cross-case synthesis compared the

threats to the GM4W and QoAir systems. We distinguished three types of threats from this comparison, namely hardware-related, software-related, and human-related threats. The key component of accessible hardware indicates whether a system has components that are prone to hardware-related threats, of which we found hardware failure and theft to be high-risk threats. The software-related threats involve more knowledge on the type of system that we assess. The two cases in this study had the same software-related components in terms of control and data processing and collecting components. The main difference between the two was the centralized data storage versus the decentralized data storage with the blockchain technology of QoAir. Security issues concerning data encryption, malicious attacks, and malware are addressed with blockchain, even though the software is still prone to failure. The GM4W had human-related threats to the system. Having staff with access to the system makes the project prone to human errors and insider attacks. By addressing each of the three categories, we can assess the risk to the system in a structured manner.

We compared the risk treatment controls as well. Creating a robust network and having backup protocols are controls identified in both assessments and general good practices for risk treatment. We found software and hardware failure in both cases as high-risk threats. The failure of key components can be mitigated with the aforementioned robust network and backup protocols. We divide human-related threats into the staff of system and outsiders. Staff training addresses the human error threat, while identity and access control mitigate theft and insider attacks. The identity and access control grants access to parts of the system, while also checking the history of who accessed the system. Software-related threats can have more specific mitigation controls, such as data encryption to secure data transferring and integrity monitoring, to ensure the validity of data.

The main research question

In conclusion, we circle back to the main research question we presented at the start of this section. We fount ound that the identified key cyber components for innovation projects benefit the identification and mitigation of cyber threats. When assessing an innovation, the cyber components serve as a starting point of the assessment. We used SecRAM as the risk assessment method in this study and aimed to test whether the method applies to the risk assessment of innovation projects. We conclude that the SecRAM method serves its purpose and applies to the innovation projects in the context of this study. The risk assessments applied to different cases with contrasting structures and enabled us to identify and mitigate cyber threats effectively.

The cases in this study revealed numerous potential threats for innovation projects in climate disaster resilience. We categorize the threats to hardware-, software-, and human-related threats. We found mitigation controls for each category, and in general terms as well. Creating a robust network and having backup protocols are controls identified in both assessments and general good practices for risk treatment. These mitigation controls apply to most of the identified risks for innovation projects.

7.2 REFLECTION

7.2.1 Research Limitations

We used a mix of methods to gather data in this study. A combination of quantitative and qualitative methods was used to gather and analyze data in different parts of the study. The use of both quantitative and qualitative methods come with various assumption and limitations. Combining the results of these methods should address the assumptions and limitation of these methods as well. The validity of results is a concern in some of the methods and discussed per method in this section.

The study used cases from the BRIGAID program. The program's portfolio contains a wide range of climate disaster resilience projects, varying in subject, hazards covered, type of innovation, and project size. Despite the variety of the portfolio, the projects were chosen based on their common goal of climate disaster resilience. Other types of innovations not covered in this study could show other results, such as other key cyber components. The conclusions of this study, especially the generalized conclusions made for innovation projects, come with the understanding and remark that these conclusions are made based on a select type of innovation project.

This limitation also affects the survey results. The sample came from a finite population, namely the innovation projects affiliated with the BRIGAID program. The limited number of responses increases the margin of error of the sample size. When interpreting the results, we must keep this margin of error in mind.

The SecRAM risk assessment uses qualitative data for the assessment of the cases. We aimed for a qualitative risk assessment due to the lack of data, especially in the case of innovation projects. This lack of data would have complicated the practicality of the study. The qualitative risk assessment comes with the notion that the risk estimations are mostly subjective of nature. This subjectivity is a concern for the validity of the assessment. Expert knowledge improves the validity of the assessment. This was not achieved in this study due to time constraint.

7.2.2 Societal Relevance

The increasing use of the cyberspace and connectivity of society has raised numerous concerns about our safety, security, and privacy. The proposed extension of the TIF tool benefits the innovation projects in preparing their systems for a safe and secured market introduction. Successful, local practices become common practices and can benefit innovations globally. This benefit helps not only the innovators but also the users of these innovations. Additionally, the data that innovations hold or use in their processes are more secured as well. The security of our data and privacy will become more important in our developing (cyber) society, and this study's results should benefit the protection of the data and privacy of society with the effective identification and mitigation of cyber threats as presented in this study. By assessing the systems of innovation projects in climate disaster resilience according to the proposed tool, we can prepare the innovators by confronting them to new insights in their systems and exposing areas of concern according to the confidentiality, integrity, and availability performance indicators.

7.2.3 Scientific Relevance

This study focused on innovation projects in climate adaptation and disaster resilience, as these are the innovation within the BRIGAID program. The self-assessment tool of BRIGAID serves the innovators in producing a more efficient development of their projects by using scientific proofed assessment methods. This study aimed to add a cybersecurity assessment to the TIF tool. We addressed the found knowledge gaps in cybersecurity of how to manage the changing risks to a system with the compilation of a cyber component list and assessment methodology. Where assessment methodologies in other fields of study are dependent on data or assess

aspects of a system irrelevant to innovation projects, we designed a cybersecurity assessment covering the key components of an innovation project's system. The risk assessment showed its applicability to systems with different structures, in this study's case, a centralized cloud environment, and a decentralized blockchain system. The small sample size and the lack of involvement of the innovators in the later stages of the assessment are limitations to the study. Nonetheless, the results showed an effective approach for the assessment of cyber-physical systems. This approach could be used as a practical road map for assessing cyber risks. The compiled list of cyber components served well in the conceptualization of systems in this study. More specific, the list identifies supporting assets of a cyber-physical system effectively and could serve future research involving a cyber risk assessment.

7.2.4 EPA Curriculum Alignment

This research aligns with the Engineering and Policy Analysis curriculum and requirements for the Master thesis. The current increasing frequency and severity of climate disasters urge innovators to come up with solutions to keep our society safe. Solutions from the covered innovation projects are not solely relevant for a single part of society, as most of the innovations can be applicable on a global scale. Both climate change and cybersecurity are grand challenges we face as a society. This research focuses on cybersecurity of innovations for climate disaster resilience because of the projects that affiliate with the BRIGAID program. However, the conclusions of this research are aimed at innovation projects on a larger scale, making cybersecurity the main grand challenge of this research. The conclusions should benefit innovators in generating more knowledge on the cybersecurity of their projects and support their decision making when risks need treatment.

7.3 RECOMMENDATIONS

7.3.1 Contribution of the Study

This study aimed for an effective way to identify and mitigate cyber threats. The study used a mix of methods to derive data from both quantitative and qualitative methods. We identified key cyber components of innovation projects from literature, interviews, and a survey to conceptualize the system of a project and identify cyber threats effectively. The cases for this study came from the BRIGAID program and gave a variety of innovation projects in climate disaster resilience. The risk assessments, according to the SecRAM method, provided us with an effective method for the identification and mitigation of cyber threats that are generally applicable. The study categorized threats in three groups, dividing software-, hardware-, and human-related threats, with treatment controls for each category. From the results, we designed a cybersecurity assessment tool that serves as an extension to the TIF assessment tool of BRIGAID. Innovators can self-assess their projects with the extension to identify cyber threats and assess their projects from a system-oriented, technical perspective.

7.3.2 Recommendations for BRIGAID

The TIF cybersecurity extension from this study is verified and validated to be of use in the current state. The extension follows the same structure as the rest of the tool and works as a standalone assessment. We recommend BRIGAIDs experts to critically reflect on the tool and determine whether the extension improves the overall tool enough to be implemented. For the validation, we use the Technology Acceptance Model (TAM) for the implementation of the proposed cybersecurity extension. The TAM aims to measure the usefulness and ease of use as perceived by the intended users. The model gives an indication of the intention to use and eventual usage of the new technology. In this study, we applied to the model to the perceptions of BRIGAIDs Project Manager. We recommend applying this validation model to a sample of innovators and partners of BRIGAID to determine their perceptions on the extension of the tool. Both the expert validation and intention to use the model help indicate whether the extension is worth implementing.

7.3.3 Recommendations for Innovators

We recommend innovators to self-assess their systems with the proposed tool extension. The tool benefits innovators in different stages of development. Addressing issues with the system early in the development cycle benefits the project by exposing threats right away and limiting the number of unaddressed risks later on in the cycle. We found the perceived importance of cybersecurity among the responding innovators to our survey to be relatively low. Some cyber threats are more obvious than others, and the likelihood and impact of the threats can be misjudged. Again, addressing these threats early on reduces the chance of surprises during the later stages of development or even after deployment. The assessment differs from the rest of the TIF tool in the perspective that we used. The current tool forces innovators to assess the project focused on the implication to the environment and the climate disaster that they address. The extension forces innovators to assess its project systematically. This different perspective conceptualizes the data flows and infrastructure within the system and can bring new insights to the innovation.

7.3.4 Recommendations for Future Research

The tools used in this study vary per method. For the web scraping of the Climate Innovation Window, we used a web tool in combination with a Python script to clean up and visualize the data. On the other hand, we used R to clean up and visualize the data from the survey. We chose R as the preferred option for data analysis and visualization. However, we used Python because of its potential improvements for the web scraping method. We now manually initiate the web scraping process and load the data in the Python script. Future studies can improve upon this method by having Python begin the web scraping process. Python has packages that can scrape data off the web, but also initiate online tools to do so. The next step in improvement is the storage of the data and updates to that storage. The connection between Python and MySQL serves as an excellent option to create a database and maintain it with periodical updates of the database.

Section 7.2.3 addressed the applicability of the risk assessment used in this study as the main takeaway from this study. Marotta et al. (2013) concluded that the applicability of SecRAM should be tested in other fields of study, and we conclude that the method is applicable to assessing innovation projects as well. We base this conclusion on a small sample size, and future research should expand upon the range of projects assessed following the SecRAM method. Involving the innovators and experts in the data-gathering phase, as we did in this study is recommended. However, the innovators' involvement could be extended to the assessment phase as well. This involvement is not addressed in this study but should be considered for future research.

Finally, we address the methodology in this study. We used a mix of both quantitative and qualitative methods. The use of numerous methods had the benefit of providing different results that apply to different parts of the study. For example, we used a literature review, expert interviews, and a survey among innovators to compile the list of key cyber components. Each method provided us with information from different perspectives. However, we found the use of a mix of methods to be challenging, especially when structuring the found data and scientifically using that data. Each method comes with its assumptions and limitations, and by drawing conclusions from different sources, we should address the combination of assumptions and limitations as well to ensure the validity of our conclusions.

BIBLIOGRAPHY

Abdel-Basset, M., Gunasekaran, M., Mohamed, M., and Chilamkurti, N. (2019). A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain. *Future Generation Computer Systems*, 90:489–502.

Alhawari, S., Karadsheh, L., Talet, A. N., and Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management*, 32(1):50–65.

Ali, B. and Awad, A. (2018). Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 18(3):817.

Anderson, J. and Bausch, C. (2006). Climate change and natural disasters: Scientific evidence of a possible relation between recent natural disasters and climate change. *Policy Department Economic and Scientific Policy*, 2.

Andrews, F. M. (1984). Construct validity and error components of survey measures: A structural modeling approach. *Public Opinion Quarterly*, 48(2):409–442.

Asgari, H., Haines, S., and Rysavy, O. (2018). Identification of threats and security risk assessments for recursive internet architecture. *IEEE Systems Journal*, 12(3):2437–2448.

Ashibani, Y. and Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81–97.

Ashok, A. and Govindarasu, M. (2015). Cyber-physical risk modeling and mitigation for the smart grid using a game-theoretic approach. In *2015 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5. IEEE.

Bahtit, H. and Regragui, B. (2013). Risk management for iso27005 decision support. *International Journal of Innovative Research in Science, Engineering and Technology*.

Baxter, P. and Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report*, 13(4):544–559.

Beggs, C. and Warren, M. (2009). Safeguarding australia from cyber-terrorism: a proposed cyber-terrorism scada risk framework for industry adoption.

Bharanipriya, V. and Prasad, V. K. (2011). Web content mining tools: a comparative study. *International Journal of Information Technology and Knowledge Management*, 4(1):211–215.

Blakley, B., McDermott, E., and Geer, D. (2001). Information security is information risk management. In *Proceedings of the 10th New Security Paradigms Workshop (NSPW)*, pages 97–104. ACM.

Blöschl, G., Hall, J., Parajka, J., Perdigão, R. A., Merz, B., Arheimer, B., Aronica, G. T., Bilibashi, A., Bonacci, O., Borga, M., et al. (2017). Changing climate shifts timing of european floods. *Science*, 357(6351):588–590.

Bowers, J. and Khorakian, A. (2014). Integrating risk management in the innovation project. *European Journal of Innovation Management*, 17(1):25–40.

BRIGAID (2016a). Our mission. `https://brigaid.eu/new_our-mission/`. Last Accessed: 30 July 2019.

BRIGAID (2016b). Technical readiness & performance indicators. `https://brigaid.eu/what-trl/`. Last Accessed: 3 August 2019.

Byres, E. J., Franz, M., and Miller, D. (2004). The use of attack trees in assessing vulnerabilities in scada systems. In *Proceedings of the International Infrastructure Survivability Workshop (IISW)*, pages 3–10. Citeseer.

Caralli, R., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). Introducing octave allegro: Improving the information security risk assessment process.

Castillo, A. (2014). Risk analysis and management in power outage and restoration: A literature survey. *Electric Power Systems Research*, 107:9–15.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. (2016). A review of cyber security risk assessment methods for scada systems. *Computers & security*, 56:1–27.

Chittester, C. G. and Haimes, Y. Y. (2004). Risks of terrorism to information technology and to critical interdependent infrastructures. *Journal of Homeland Security and Emergency Management*, 1(4).

Chockalingam, S., Pieters, W., Teixeira, A., and van Gelder, P. (2017). Bayesian network models in cyber security: a systematic review. In *Proceedings of the 22nd Nordic Conference on Secure IT Systems (NordSec)*, pages 105–122. Springer.

CIOReview (2016). Risks related to data storage and importance of its management. https://www.cioreview.com/news/risks-related-to-data-storage-and-importance-of-its-management-nid-18522-cid-141.html. Last Accessed: 20 August 2019.

Craigen, D., Diakun-Thibault, N., and Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Custódio, C., Ferreira, M. A., and Matos, P. (2017). Do general managerial skills spur innovation? *Management Science*, 65(2):459–476.

Dai, F., Shi, Y., Meng, N., Wei, L., and Ye, Z. (2017). From bitcoin to cybersecurity: A comparative study of blockchain application and security issues. In *Proceedings of the 4th International Conference on Systems and Informatics (ICSAI)*, pages 975–979. IEEE.

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8):982–1003.

Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management.

Edwards-Schachter, M. (2018). The nature and variety of innovation. *International Journal of Innovation Studies*.

Elbeck, M. (2014). Selecting a free web-hosted survey tool for student use. *e-Journal of Business Education and Scholarship of Teaching*, 8(2):54–68.

Environmental Protection Agency (2014). Keeping your cool: how communities can reduce the heat island effect. (Publication No. 430F14041). Retrieved from https://www.epa.gov/heat-islands/heat-island-outreach-materials.

Fabian, B., Gürses, S., Heisel, M., Santen, T., and Schmidt, H. (2010). A comparison of security requirements engineering methods. *Requirements Engineering*, 15(1):7–40.

Farahmand, F., Navathe, S. B., Enslow, P. H., and Sharp, G. P. (2003). Managing vulnerabilities of information systems to security incidents. In *Proceedings of the 5th International Conference on Electronic Commerce (ICEC)*, pages 348–354. ACM.

Forzieri, G., Bianchi, A., e Silva, F. B., Herrera, M. A. M., Leblois, A., Lavalle, C., Aerts, J. C., and Feyen, L. (2018). Escalating impacts of climate extremes on critical infrastructures in europe. *Global Environmental Change*, 48:97–107.

Forzieri, G., Cescatti, A., e Silva, F. B., and Feyen, L. (2017). Increasing risk over time of weather-related hazards to the european population: a data-driven prognostic study. *The Lancet Planetary Health*, 1(5):e200–e208.

Galletta, A. (2013). *Mastering the semi-structured interview and beyond: From research design to analysis and publication*, volume 18. NYU press.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., and Linkov, I. (2017). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*.

Gerring, J. (2004). What is a case study and what is it good for? *American Political Science Review*, 98(2):341–354.

Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., and Halderman, J. A. (2014). Green lights forever: Analyzing the security of traffic infrastructure. In *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT)*.

Giraldo, J., Sarkar, E., Cardenas, A. A., Maniatakos, M., and Kantarcioglu, M. (2017). Security and privacy in cyber-physical systems: A survey of surveys. *IEEE Design & Test*, 34(4):7–17.

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., and Linkov, I. (2017). Resilience of cyber systems with over-and underregulation. *Risk Analysis*, 37(9):1644–1651.

GReD (2018). Geoguard. https://www.g-red.eu/geoguard/. Last Accessed: 16 August 2019.

Hart, C., Feenberg, A., et al. (2014). The insecurity of innovation: A critical analysis of cybersecurity in the united states. *International Journal of Communication*, 8:19.

Hellström, T. (2003). Systemic innovation and risk: technology assessment and the challenge of responsible innovation. *Technology in Society*, 25(3):369–384.

Henry, M. H. and Haimes, Y. Y. (2009). A comprehensive network security risk model for process control networks. *Risk Analysis: An International Journal*, 29(2):223–248.

Hughes, J. and Cybenko, G. (2013). Quantitative metrics and risk assessment: The three tenets model of cybersecurity. *Technology Innovation Management Review*, 3(8).

Hutchison-Krupat, J. and Chao, R. O. (2014). Tolerance for failure and incentives for collaborative innovation. *Production and Operations Management*, 23(8):1265–1285.

Jalali, S. and Wohlin, C. (2012). Systematic literature studies: database searches vs. backward snowballing. In *Proceedings of the 6th ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, pages 29–38. IEEE.

Joint Task Force Transformation Initiative (2012). Guide for conducting risk assessments. Technical report, National Institute of Standards and Technology.

Jonkman, S. N., Stive, M. J., and Vrijling, J. K. (2005). New orleans is a lesson to the dutch. *Journal of Coastal Research*, pages xi–1191.

Kahn, M. E. (2005). The death toll from natural disasters: the role of income, geography, and institutions. *Review of Economics and Statistics*, 87(2):271–284.

Karabacak, B. and Sogukpinar, I. (2005). Isram: information security risk analysis method. *Computers & Security*, 24(2):147–159.

Kettani, H. and Wainwright, P. (2019). On the top threats to cyber systems. In *Proceedings of the 2nd International Conference on Information and Computer Technologies (ICICT)*, pages 175–179. IEEE.

Komninos, N., Philippou, E., and Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954.

Kong, H.-K., Hong, M. K., and Kim, T.-S. (2018). Security risk assessment framework for smart car using the attack tree analysis. *Journal of Ambient Intelligence and Humanized Computing*, 9(3):531–551.

Labunets, K., Massacci, F., Paci, F., Marczak, S., and de Oliveira, F. M. (2017). Model comprehension for security risk assessment: an empirical comparison of tabular vs. graphical representations. *Empirical Software Engineering*, 22(6):3017–3056.

Leichenko, R. (2011). Climate change and urban resilience. *Current Opinion in Environmental Sustainability*, 3(3):164–168.

Lin, I.-C. and Liao, T.-C. (2017). A survey of blockchain security issues and challenges. *IJ Network Security*, 19(5):653–659.

Liu, J., Xiao, Y., Li, S., Liang, W., and Chen, C. P. (2012). Cyber security and privacy issues in smart grids. *IEEE Communications Surveys & Tutorials*, 14(4):981–997.

Loreau, M., Naeem, S., Inchausti, P., Bengtsson, J., Grime, J., Hector, A., Hooper, D., Huston, M., Raffaelli, D., Schmid, B., et al. (2001). Biodiversity and ecosystem functioning: current knowledge and future challenges. *Science*, 294(5543):804–808.

Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I. (2015). Internet of things (iot) security: Current status, challenges and prospective measures. In *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341. IEEE.

Mankins, J. C. (2009). Technology readiness assessments: A retrospective. *Acta Astronautica*, 65(9-10):1216–1223.

Marotta, A., Carrozza, G., Battaglia, L., Montefusco, P., and Manetti, V. (2013). Applying the secram methodology in a cloud-based atm environment. In *Proceedings of the 8th International Conference on Availability, Reliability and Security (ARES)*, pages 807–813. IEEE.

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., and Frye, J. (2012). Cyber threat metrics. *Sandia National Laboratories*.

Mell, P., Scarfone, K., and Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, 4(6):85–89.

Mihić, M., Dodevska, Z., Todorović, M., Obradović, V., and Petrović, D. (2018). Reducing risks in energy innovation projects: Complexity theory perspective. *Sustainability*, 10(9):2968.

Nam, T. and Pardo, T. A. (2011). Smart city as urban innovation: Focusing on management, policy, and context. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance (ICEGOV)*, pages 185–194. ACM.

Nemoto, T. and Beglar, D. (2014). Likert-scale questionnaires. In *Proceedings of the 19th Japan Association for Language Teaching Conference (JALT)*, pages 1–8.

NIST (2002). 800-30 risk management guide for information technology systems. *National Institute for Standards and Technology*.

NIST (2011). Guide for applying the risk management framework to federal information systems: A security life cycle approach, nist special publication 800-37 (rev 1).

Oleson, K., Monaghan, A., Wilhelmi, O., Barlage, M., Brunsell, N., Feddema, J., Hu, L., and Steinhoff, D. (2015). Interactions between urbanization, heat stress, and climate change. *Climatic Change*, 129(3-4):525–541.

Olwig, M. F. (2012). Multi-sited resilience: The mutual construction of "local" and "global" understandings and practices of adaptation and innovation. *Applied Geography*, 33:112–118.

Owusu, P. A. and Asumadu-Sarkodie, S. (2016). A review of renewable energy sources, sustainability issues and climate change mitigation. *Cogent Engineering*, 3(1):1167990.

Patel, S. C., Graham, J. H., and Ralston, P. A. (2008). Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements. *International Journal of Information Management*, 28(6):483–491.

Patel, S. C. and Zaveri, J. (2010). A risk-assessment model for cyber attacks on information systems. *Journal of Computers*, 5(3):352–359.

Pearson, I. L. (2011). Smart grid cyber security for europe. *Energy Policy*, 39(9):5211–5218.

Pelling, M. (2010). *Adaptation to climate change: from resilience to transformation*. Routledge.

Peng, Y., Lu, T., Liu, J., Gao, Y., Guo, X., and Xie, F. (2013). Cyber-physical system risk assessment. In *Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pages 442–447. IEEE.

Permann, M. R. and Rohde, K. (2005). Cyber assessment methods for scada security. Technical report, Idaho National Laboratory (INL).

Pfleeger, S. L. and Kitchenham, B. A. (2001). Principles of survey research: part 1: turning lemons into lemonade. *ACM SIGSOFT Software Engineering Notes*, 26(6):16–18.

Purdy, G. (2010). Iso 31000: 2009—setting a new standard for risk management. *Risk Analysis: An International Journal*, 30(6):881–886.

Radanliev, P., De Roure, D., Nurse, J., Montalvo, R. M., and Burnap, P. (2019). Standardisation of cyber risk impact assessment for the internet of things (iot). *arXiv preprint arXiv:1903.04428*.

Radanliev, P., De Roure, D. C., Nicolescu, R., Huth, M., Montalvo, R. M., Cannady, S., and Burnap, P. (2018). Future developments in cyber risk assessment for the internet of things. *Computers in Industry*, 102:14–22.

Ralston, P. A., Graham, J. H., and Hieb, J. L. (2007). Cyber security risk assessment for scada and dcs networks. *ISA Transactions*, 46(4):583–594.

Refsdal, A., Solhaug, B., and Stølen, K. (2015). Cyber-risk management. In *Cyber-Risk Management*, pages 33–47. Springer.

Rica, M., Bea, M., Lopez Gunn, E., and Santos, P. (2017). How to enhance innovations for climate disaster resilience through brigaid (policy brief 04-17). Retrieved from `https://brigaid.eu/public-deliverables/`.

Rohat, G., Flacke, J., Dosio, A., Pedde, S., Dao, H., and van Maarseveen, M. (2019). Influence of changes in socioeconomic and climatic conditions on future heat-related health challenges in europe. *Global and Planetary Change*, 172:45–59.

Ross, R. S. (2011). Managing information security risk: Organization, mission, and information system view — nist. Technical report.

Ruegamer, A. and Kowalewski, D. (2015). Jamming and spoofing of gnss signals–an underestimated risk?! In *Proc. Wisdom Ages Challenges Modern World*, pages 17–21.

Sale, J. E., Lohfeld, L. H., and Brazil, K. (2002). Revisiting the quantitative-qualitative debate: Implications for mixed-methods research. *Quality and Quantity*, 36(1):43–53.

Saripalli, P. and Walters, B. (2010). Quirc: A quantitative impact and risk assessment framework for cloud security. In *Proceedings of the 3rd International Conference on Cloud Computing (CLOUD)*, pages 280–288. IEEE.

Satorra, A. and Bentler, P. M. (2001). A scaled difference chi-square test statistic for moment structure analysis. *Psychometrika*, 66(4):507–514.

Schonlau, M. and Couper, M. P. (2016). Semi-automated categorization of open-ended questions. In *Survey Research Methods*, volume 10, pages 143–152.

Sebastian, A., Lendering, K., van Loon-Steensma, J., Paprotny, D., Bellamy, R., Willems, P., van Loenhout, J., and Colaço, M. (2019a). A Test and Implementation Framework (TIF-Tool) for Climate Adaption Innovations: Tool Guidance. Technical report, BRIGAID.

Sebastian, A., van Loon-Steensma, J., and Bellamy, R. (2019b). A test and implementation framework (tif-tool) for climate adaption innovations: Tool guidance. Technical report, BRIGAID.

SESAR (2013). Sesar atm secram implementation guidance material. *SESAR Joint Undertaking Project 16.02.03*, page D03. Retrieved from `http://www.sesarju.eu/`.

Singer, P. W. and Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. OUP USA.

Song, J.-G., Lee, J.-W., Lee, C.-K., Kwon, K.-C., and Lee, D.-Y. (2012). A cyber security risk assessment for the design of i&c systems in nuclear power plants. *Nuclear Engineering and Technology*, 44(8):919–928.

Stergiopoulos, G., Gritzalis, D., and Kouktzoglou, V. (2018). Using formal distributions for threat likelihood estimation in cloud-enabled it risk assessment. *Computer Networks*, 134:23–45.

Stouffer, K. A., Falco, J. A., and Scarfone, K. A. (2011). Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc).

Sun, C.-C., Hahn, A., and Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, 99:45–56.

SurveyGizmo (2005). Surveygizmo survey software. *SurveyGizmo Boulder, CO*. `http://www/surveygizmo.com`. Last Accessed: 21 August 2019.

Tellis, W. M. (1997). Application of a case study methodology. *The Qualitative Report*, 3(3):1–19.

Torkura, K. A., Cheng, F., and Meinel, C. (2015). A proposed framework for proactive vulnerability assessments in cloud deployments. In *Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 51–57. IEEE.

Van Aalst, M. K. (2006). The impacts of climate change on the risk of natural disasters. *Disasters*, 30(1):5–18.

Van de Ven, A. H. (1986). Central problems in the management of innovation. *Management science*, 32(5):590–607.

van Loon-Steensma, J. M. (2018). The potential of brigaid's testing and implementation framework (tif) as a tool to promote nature based solutions. In *EGU General Assembly Conference Abstracts*, volume 20, page 10374.

Vargas-Hernández, J. G., Noruzi, M. R., and Sariolghalam, N. (2010). Risk or innovation, which one is far more preferable in innovation projects? *International Journal of Marketing Studies*, 2(1):233.

Vargiu, E. and Urru, M. (2013). Exploiting web scraping in a collaborative filtering-based approach to web advertising. *Artificial Intelligence Research*, 2(1):44–54.

Veeramany, A., Hutton, W. J., Sridhar, S., Gourisetti, S. N. G., Coles, G. A., and Skare, P. M. (2019). A framework for development of risk-informed autonomous adaptive cyber controllers. *Journal of Computing and Information Science in Engineering*, 19(4):041004.

Verendel, V. (2009). Quantified security is a weak hypothesis: a critical survey of results and assumptions. In *Proceedings of the 18th New Security Paradigms Workshop (NSPW)*, pages 37–50. ACM.

Vitunskaite, M., He, Y., Brandstetter, T., and Janicke, H. (2019). Smart cities and cyber security: Are we there yet? a comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*, 83:313–331.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38:97–102.

Wang, J., Lin, W., and Huang, Y.-H. (2010). A performance-oriented risk management framework for innovative r&d projects. *Technovation*, 30(11-12):601–611.

WebScraper (2019). Making web data extraction easy and accessible for everyone. `https://webscraper.io/`. Last Accessed: 21 August 2019.

Webster, J. and Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, pages xiii–xxiii.

Wilhelmi, O. V. and Hayden, M. H. (2010). Connecting people and place: a new framework for reducing urban vulnerability to extreme heat. *Environmental Research Letters*, 5(1):014021.

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., and Clausen, L. (2011). Threat assessment & remediation analysis (tara): Methodology description version 1.0. Technical report, MITRE CORP BEDFORD MA.

Yin, R. K. (2003). Case study research: Design and methods. *Sage Publications, Inc*, 5:11.

Yin, R. K. (2011). *Applications of case study research*, chapter A (very) brief refresher on the case study method. Sage.

Zhang, Y. and Wildemuth, B. M. (2009). Qualitative analysis of content. *Applications of Social Research Methods to Questions in Information and Library Science*, 308:319.

APPENDICES

A | INTERVIEW PROCEDURE

A.1 PROCEDURE

I want to start by thanking you for your time and effort with participating in this interview. With your consent, the interview will be recorded to prevent disruptions in the conversation as much as possible. Interview results will be presented in the thesis, I will personally send each interviewee a digital copy, if defended successfully. The expected duration of the interview is approximately 30 minutes.

I am currently working on my master's thesis, which is a study on how to assess cybersecurity specifically for innovation projects. The cybersecurity of innovation projects has unique components which I have tried to identify through a literature review. This resulted in a list of cyber components, which I want to validate through interviews with experts in the field of innovation projects or relatable fields of study. I am interested in your approach to the cybersecurity of your system(s) and what elements, vectors, or components you see as crucial when assessing (cyber)risks. On the page below you will find the list of components I have identified through the literature review.

A.2 QUESTIONS

1. How do you describe your role in your company?
2. How would you describe your company's cybersecurity efforts?
3. Do you believe that innovation projects are unique when assessing cybersecurity?
4. What are your most important Lessons Learned when assessing cybersecurity of innovation projects?
5. What do you consider to be the most important knowledge gap of cybersecurity of innovation projects?
6. In the proposed list of cyber components, five categories are defined.
    a) In your view, do these five categories cover the important components of a system?
    b) What adjustments would you make to these categories?
    c) What do you consider to be the most important category?
7. Most innovation projects consist of a cyber-physical system. Is the physical element a vital part of the cybersecurity of your system?
8. Can you name three key components of cybersecurity?
9. Do you believe that the key components are different when focusing on innovation projects specifically?
10. Are there any specific components (/elements/assets) that, in Your view, are key to the cybersecurity of innovation projects and missing or not covered properly on this list?

a.3 CYBER COMPONENT LIST

Cyber Components of Innovation Projects

Data collection - Components that collect data in the physical world

- Real-time data (e.g., Meteorological sensor, Real-time Business Intelligence)
- Smart meters (e.g., Electricity/Gas/Water meter, Load Control)
- Cameras (e.g., Closed-circuit television)
- Other types of sensors, namely:
- Other data collecting component(s) not on the list, namely:

Communication - Components which enable communication between components in a system or between separate systems

- Communication through landline, power grid line
- Communication through mobile line (GSM, 3G, 4G)
- Communication through satellite (GPS)
- Human Machine Interface (e.g., Automated assistance, Equipment/Machinery Monitoring, Electronic Display)
- Other communication component(s) not on the list, namely:

Data processing - Components that either store collected data or perform some type of action based on data collecting components

- Autonomous decision-making (e.g., Decision-making algorithms, Machine learning)
- Other actuators, namely:
- Data processing/analysis tools (e.g., spreadsheet, data visualization, raw data)
- Cloud technologies
- Offline data storage
- User Interface (e.g., Operating system, programming environment)
- Other data processing component(s) not on the list, namely:

Control - Components that control the physical components of a system and monitor performances

- Servers
- Firewalls
- Anti-viruses
- Feeder protection relays
- Malfunction Management Units
- Other control component(s) not on the list, namely:

Physical - Components that are placed in or part of the physical world

- Accessible hardware (for insiders only) (e.g., in-office servers, hardcopy data, on-site setups)
- Accessible hardware (for outsiders) (e.g., equipment physically accessible for outside attackers/intruders, off-site setups)
- Network access points / Points of entry
- (Ecological) Environment that can affect hardware (e.g., equipment prone to erosion/wear tear/extreme weather)
- Other physical component(s) not on the list, namely:

A.4 INTERVIEW DATA

We use a word table to structure the qualitative data from the interviews (see Table A.1). It is a form of coding for the gathered data from the interviews to ensure the replicability of the research. We distinguish the main concepts as the primary level words. We structure these main concepts with underlying concepts, which we present as secondary level concepts. Certain secondary level concepts have underlying concepts themselves, creating a final, tertiary level of ideas from the interview results. Table A.1 has a fourth column, which provides a brief explanation of the concept.

Table A.1: Three-level word table as a presentation of concepts from the interviews

Level			
Primary	**Secondary**	**Tertiary**	**Theme**
Cybersecurity			From what perspective do you look at cybersecurity
	Technical		Technical perspective focuses on the separate components of a system, and what connection to the system are possible
	Process		The process perspective focuses on the main communication line, and from there explain the system
	Policy		Policy's perspective is focusing on the governance of the system, seems lacking in innovation
		Personal data	Personal data is valuable and needs protection, which is monitored by law
	Physical		This perspective looks at components as physical, tangible products, such as machines
	Data Flow		This perspective focuses on data traffic, where is data coming from and going to
	Security Concepts		The security concepts of information security
		Confidentiality	Are the information and services disclosed to serve only authorized entities

Continued on next page

Table A.1 – continued from previous page

Primary	Secondary	Tertiary	Theme
		Integrity	Are the information and services provided accurate and complete
		Availability	Are the information and services available at all times, or when demanded
System			How can we define and frame a system, different components can be identified
	People		People play a role when entering the system,affecting its process
		Identity	Who is entering the system
		Authorization	What can you do in the system
		Authentication	What do you know, what information affecting the system do you have
		Accountability	What are your roles and responsibilities in the system
	Components		Individual components can be distinguished in a system
		Incoming	What is the input for a component does it require information or services
		Communication	How is the component communicating with other parts of the system
		Outgoing	What information about services is provided by the component
		Location	Where is the component placed, is it accessible
	Infrastructure		The infrastructure of the system can be both physical as cyber
		Middleware	Software that connects hardware to databases or the main operating system
		Software	Data or instructions for components to operate
		Components	Physical assets of the infrastructure, using middleware and software in their processes
		Hardening	Concept of eliminating all information and services that are not needed or can be reduced
	Communication		Communication between components ensures the exchange of information and services
		Ports	Ports are entrances to the communication lines of a system, often protected by a firewall
		Servers	Servers are the entities that are sending and receiving information through the communication line

Continued on next page

Table A.1 – continued from previous page

Primary	Secondary	Tertiary	Theme
		Encryption	Encryption takes data an puts a protective layer on or creates a protected communication line for data to travel over
		Protocols	Protocols are layers used to communicate over the internet
		Internet	The internet is a communication line, which has numerous layers to describe the communication
		Access point	Physical points of entry of the system, such as a router for internet communication
	Encryption		Encrypting data can be done in several ways, different parts of a system need encryption
		Data	Data, like an e-mail or instant messages, can be encrypted by encoding them before sending
		Communication line	Data can be sent through an encryption tunnel, protecting it from outsiders' eyes
		Database	Storages of data can be accessed through communication, and need protection after data is unpacked and stored
		Passwords	Passwords grant access to a system, encrypting passwords storages and communication increases the security
	Security		Security of a system can be approached in different ways, themes of system security are defined
		Framework	A framework for security is a standard, each new system or project can be assessed by the same framework
		Experience	Experience is identified as a critical factor, as experience in the field provides tacit knowledge like situation recognition
		Resources	Funding and man power are needed resources to ensure the safety of a system
	Rules & regulation		With data comes privacy and protective measures set by public authorities
		GDPR	European law for personal data protection
		Information usage	Information cannot be used without consent of the rightful owner, protected under law
		Illegal sale	Information, like personal data and system vulnerabilities, are valuable and sold on the black market
Governance			Systems are controlled by an overarching governing authority

Continued on next page

Table A.1 – continued from previous page

Primary	Secondary	Tertiary	Theme
	Risk Appetite		How much risk are you willing to accept
		Impact	The impact of a risk, if it would occur
		Likelihood	the likelihood of a risk to occur
	Incident management		How to manage risks that are occurring
		ITIL	Processes standard for IT systems
		Agile	Strategy popular in businesses, focussing on delivering products to clients as efficient as possible
	VSM		Visual Security Management
		Suppliers	Do you know who the suppliers of your components are, and how secure they operate
		Vendor Lock-in	Concept of using a single supplier for all your needs, simplifies VSM
	BCM		Business Continuity Management
		Strategy	How are you ensuring the continuity of the system and its processes
		Back-up	What is the plan if processes or part of the system is inactive
		Key deliverable	What are the most important information or services you need to deliver to remain operable

End of the table

B | CLIMATE INNOVATION WINDOW DATABASE

B.1 CLIMATE INNOVATION WINDOW

This appendix discusses the database creation of the innovation projects in greater detail than it is in Section 3.1.3. The establishment of the database on the innovation projects is focused on the Climate Innovation Window as created by BRIGAID. The window is a web-based collection of all the innovation projects on climate disaster resilience which are in some way associated with the BRIGAID program. The website allows users to log in and communicate directly with innovators, while all the necessary information is available. Each innovation has a unique page where all available information on the project is provided, including public documents and a direct link to the innovator's website.

We structure the appendix in the same order as the database creation process Figure B.1. First, we mined the web content from the Climate Innovation Window with a web scraping tool. Second, we cleaned the data and structured the results into a database, with visualizations of the descriptive data in Python. Lastly, we present the database.

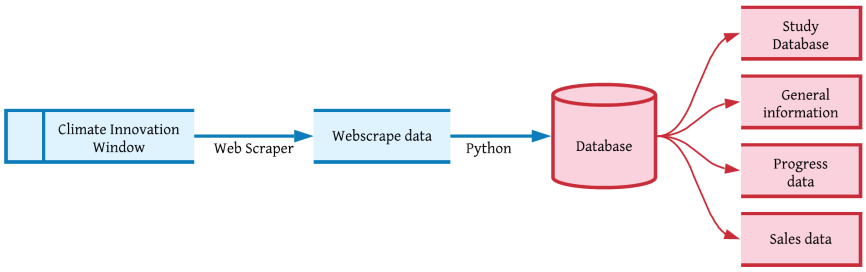


Figure B.1: The process of the database creation

B.2 WEB SCRAPING

The first step in storing the data from the /acciw is web scraping the data off of the website. Web scraping is a collection of methods and techniques that serve as automatic data gatherers. Web scrapers are particularly useful to structure data from the web into a database (Vargiu and Urru, 2013). We use the web scraping technique for web content mining. Web content mining differs from text mining in the sense that text mining involves unstructured text, whereas web content provides (semi-)structured text (Bharanipriya and Prasad, 2011). The CIW provides structured web content, i.e. we structure the content on the innovation pages in specific text categories. Figure B.2 shows the categories of texts that we identified and extracted from the innovations' web pages to store in our database.

The web scraping process starts at the homepage of the CIW. This page is the site map which is the root of the scraping process. All actions initiate from this root. If a new sequence starts, the tool must start from this site map onwards. From the homepage, the scraping tool looks for innovation-links. These are predetermined links to the unique innovation pages. Since the homepage doesn't load all of the innovation links at once, we order the tool to open all pages. We manually inspected the site and found thirteen pages of innovation page links. On these innovation pages, the scraping tool has predetermined selectors. Each type of data that

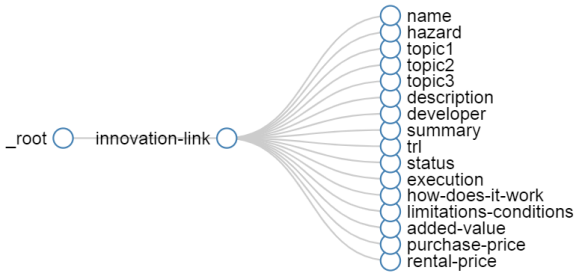


Figure B.2: Web scraping selector steps

the tool finds on the page has a selector. The CIW is structured, so each kind of information locates in the same place on all innovation pages.

After structuring the scraping selector process, we initialize the tool, and it scrapes data to a CSV-file. The data within this file is cleaned and visualized in the next step.

B.3 PYTHON SCRIPT

We load the web scraped data into the python environment. We provide Python with the data, and the script should clean this data, visualize the descriptive data, and export the newly created databases. Algorithm B.1 the pseudo-code snippet of the data cleanup. We list the used packages before initializing the data cleanup. The process starts with the CSV-file containing the web content. The data is retrieved and structured in a pandas data frame. The column headers, originally the name of the selector from the web scraping tool, are renamed for clarity. The code mines TRL categories as a string, such as "TRL 3". To create an integer column, the "TRL " (including space) is removed from the values, leaving solely the number which represents the level. Now we have an integer value. Now the data frame is clear, we can distinguish the data tables that we desire. We form four data frames by assigning the specific columns from the original data frame to each of the new data frames.

Lastly, we create the database, which is an Excel-file, with four sheets. Each of them contains a data table that holds a different type of data. The first one will provide the data that we use in this study, which includes the TRL, Hazard, and Topics, and the innovation's name as the index. The second data table contains general information of the innovation, including a brief description of the innovation and the innovator behind it. The third data table focuses on the progress of the innovation, again the TRL is included, and presents the status with BRIGAID's involvement. Lastly, there is sales data, with the provided information on the innovation, including the added value and limitations of the project. The data frame presents purchase and rental prices as provided. Table B.1 shows the full breakdown of the data tables.

The second part of the Python code visualizes the descriptive statistics for the TRL, Hazard categories, and Topic categories. Algorithm B.2 shows the pseudo-code for this visualization. The packages pandas, numpy, and mathplotlib are again used, as both Algorithm B.1 and Algorithm B.2 are snippets from one python file. For the TRL we made a bar chart Figure B.3. For the Hazard and Topic categories, both a horizontal bar chart (respectively Figure B.4 and Figure B.6) and a pie chart (respectively Figure B.5 and Figure B.7) are formed to visualize the results.

Algorithm B.1: Pseudo code of the python data cleanup and database export

```
Load in packages; pandas, numpy, mathplotlib;

Load in the database;
data = climate-innovation-window.csv
df = dataframe of data with columns 'hazard','topic1','topic2',
  'topic3','description','developer','summary','trl','status',
  'execution','how-does-it-work','limitations-conditions',
  'added-value','purchase-price','rental-price' included
Renaming the column headers for clarity

TRL Level is expressed as an integer instead of a float;

Databases are created for different purposes;
        df1 is input data for the study on representative projects
        df2 is a database for general information on the projects
        df3 contains information focusing on the progress of the projects
        df4 is a database with information for end sale purposes

while write in excel file do
    df1 as sheet 'Study data'
    df2 as sheet 'General info'
    df3 as sheet 'Project progress'
    df4 as sheet 'Sale info'
end
```

Table B.1: Categories covered per data table

Database	Name	Hazard	Topics	Description	Developer	Summary	TRL	Status	Execution	How does it work?	Limitations/conditions	Added value	Purchase price	Rental price
Study database	✓	✓	✓				✓							
General information	✓	✓	✓	✓	✓									
Progress data	✓					✓	✓	✓	✓					
Sales data	✓									✓	✓	✓	✓	✓

Algorithm B.2: Pseudo code of the python data visualization

```
visualizatuion of the TRL;
trl_list = column 'TRL' of df as a list
trl_plot = plot for the 'TRL' colums
histogram plot of trl_list
Save plot as png file

visualizatuion of the Hazards;
hazards_count = pivot table of the count value of the 'Hazards' column in df
hazards = dataframe of pivot table 'hazard_count'

horizontal bar chart plot of 'hazards'
Save plot as png file

pie chart plot of 'hazards'
Save plot as png file

visualizatuion of the Topics;
topic1_count = pivot table of the count value of the 'Topic (1)' column in df
topic1 = dataframe of pivot table 'topic1_count'
topic2_count = pivot table of the count value of the 'Topic (2)' column in df
topic2 = dataframe of pivot table 'topic2_count'
topic3_count = pivot table of the count value of the 'Topic (3)' column in df
topic3 = dataframe of pivot table 'topic3_count'
topic = concatenate topic1,topic2,topic3 in one dataframe
        fill all n/a values as 0
        make all columns integer types
topic['Count'] = topic['Count (1)'] + topic['Count (2)'] + topic['Count (3)']
        make 'Count' contain integer values horizontal bar chart plot of 'topic'

Save plot as png file

pie chart plot of 'topic'
Save plot as png file
```

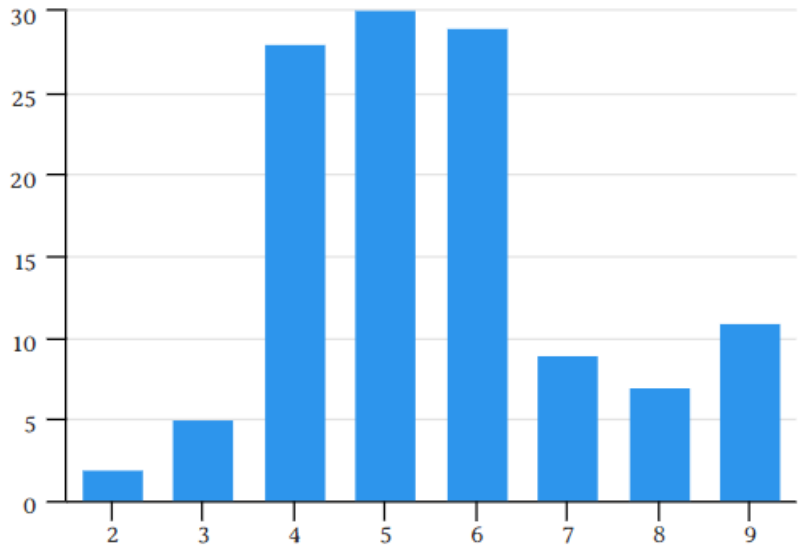


Figure B.3: Number of innovations per TRL category

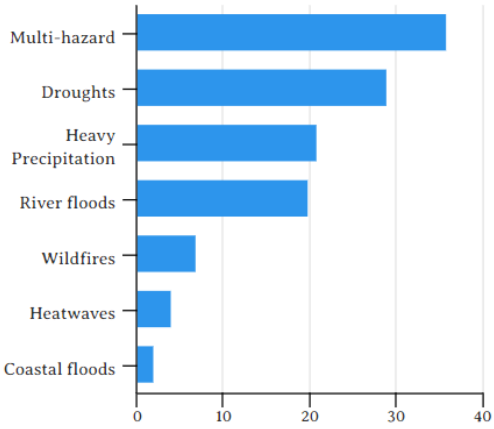


Figure B.4: Number of innovations per hazard type

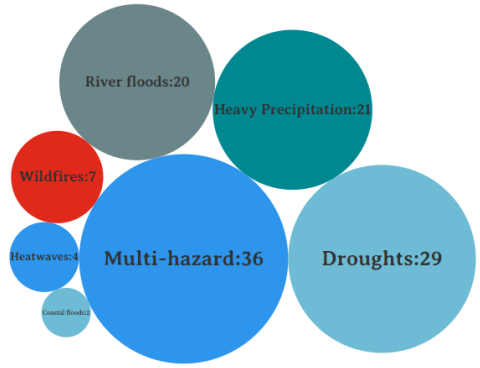


Figure B.5: Proportion of innovations per hazard

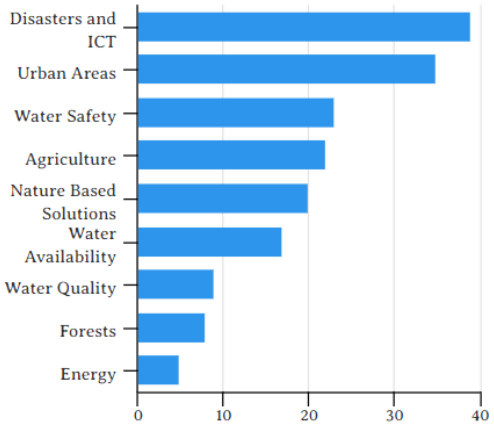


Figure B.6: Number of innovations per topic category

Figure B.7: Proportion of innovations per topic

C INNOVATOR SURVEY

This appendix presents the survey of cyber components among innovation projects in its entirety. We report the questions, as shown in the online survey. After the survey questions, we present the results from the survey among the innovators. The results include the code table, which shows the translation from survey questions to numerical values. Lastly, we present the pseudo-code for the data analysis in R.

C.1 INTRODUCTION

Cyber Components

The goal of this survey is to acquire insight into the cyber components that are specifically applicable to innovation projects when assessing cybersecurity. We define cyber components as specific parts of a system that perform a single action within that system and its cyberspace. The projects within the BRIGAID portfolio are used to validate the current list and add new components that were not identified in the literature review phase. The results will solely be used for this study. Your answers and the results will not be shared outside the research group of BRIGAID and Delft University of Technology.

I want to thank you beforehand with the time and effort you put into this survey.

Question 1 *What is the name of your innovation project?*

Question 2 *If your project was missing on the list, please provide the name below*

Question 3 *How important is cybersecurity for your innovation project?*

Question 4 *How satisfied are you with the current efforts concerning the cybersecurity of your innovation project?*

C.2 CYBER COMPONENT CATEGORIES

The next set of questions concern the cyber components of your project's system. We have defined a set of cyber components and categorized these based on our literature review. Per category, we will provide you with a list of components. We ask you to select the components which are relevant to your project's system. Lastly, we will ask you to provide us with new components, if there is any component you feel that are relevant to that category and to the cybersecurity of your system.

The categories of components are:

1. Communication: Components which enable communication between parts of a system or between separate systems.
2. Control: Components that control the physical elements of a system and monitor performances
3. Data collection: Components that collect data through physical objects

4. Data processing: Components that either store collected data or perform some type of action based on data collecting components

5. Physical: Components that are placed in or part of the physical world

Question 5 *Given the categories of cyber components from above, are there any type of components that are missing on this list? If so, please state the missing category and briefly describe the category of cyber components.*

C.3 CYBER COMPONENTS

Each category has a set of components. You are asked to check the components which are present in your project's system, Each question also has the option to add components, which you think are missing and relevant to that category.

Question 6 *My project's system has the following communication components:*

Question 7 *My project's system has the following control components:*

Question 8 *My project's system has the following data collecting components:*

Question 9 *My project's system has the following data processing components:*

Question 10 *My project's system has the following physical components:*

Question 11 *In your opinion, how would you rank the categories, given the components in that category, going from most important to least important to the cybersecurity of your project?*
(Communication, Control, Data collection, Data processing, Physical components)

Question 12 *Do you have any remarks or recommendations on the cyber components in this survey or any relevant lessons learned from your cybersecurity efforts?*

Question 13 *Lastly, if you are interested in discussing your cybersecurity efforts in greater detail, please provide your contact details below (e.g., name, phone number, e-mail). Again, this will not be shared outside this research.*

C.4 SURVEY RESULTS

The previous section showed the survey as we presented it to the innovators. We code the responses to the questions into numerical values to analyze the results. Table C.1 presents the code table of this survey. Algorithm C.1 presents the pseudo code of the R script that we use to clean and visualize the data. Note that for the thesis, we manually edited the figures to keep the figures and tables in line with the rest of the report.

We assess the number of projects that responded to the survey. We divide the responses into the type of hazard covered by the project (Figure C.1) and the topics of the projects (Figure C.2). We find a significant number of projects covering drought as a hazard in the response pool. From the database of the complete pool of innovation projects, drought was the second most frequent covered hazard, behind multi-hazard projects. The multi-hazard projects are on a shared second place with the heavy precipitation projects in our response pool. Note that the total number of topics is greater than the number of hazards covered because projects can have multiple topics. Agriculture is the most occurring topic in the response pool, followed by 'Disasters and ICT' and 'Urban Areas'. These three topics stand out from other topics in terms of occurrence. In the general pool of projects, these topic are also among the most reported innovation topics.

We have measured the composition of the innovation projects' systems according to the compiled list of cyber components. Respondents were asked to select the components which are present in their system. We gave the respondents the freedom to add categories and com-

ponents which they deem important in their system. Table C.3 presents the components as proposed by the respondents. We assess the proposed components, and decide whether we adopt the component to the list, merge several entries into one component or add an entry to an existing component. The classification column in Table C.3 shows how the entries of respondents are classified. 'Internet' and 'GPRS' are both communication lines, and make use of the mobile line we represented with the 'communication through mobile line' component. GPS data and GIS are different systems that we did not include in the proposed cyber components list. Therefore, we add these as new components. We do the same for 'mechanical components', which differ from the hardware components we present in the list by the specific function they have. We can see the 'drones' component as a data collecting smart sensor. However, within innovation projects and the technical developments, drones can become more than "regular" smart meter and have multiple features that make them unique as a component. Therefore, we added 'drones' as a new component, as well. The final new component we added from the respondents' entries is 'manually entered data'. A total of four innovation projects added some manual data gathering as another component, which is a relatively high count for such a small sample size. Lastly, one innovator added 'just a simple data structure' as another component. We see this resembling a data storage structure and assume by the term "simple" that this is an offline data storage, which is already a component in the cyber component list.

We present the most occurring components in Table C.2. While we conclude that the categories are not of the main importance, we present the number of occurring components per category (see Figure C.4). The most occurring component is the data processing/analysis tool. Most projects use some data processing tool. The survey did not ask in detail what this tool entails. The second component in terms of occurrence is 'Human-Machine Interface'. This communication component occurs in the same number of projects as 'Servers' and 'Accessible hardware (for insiders)'. To identify key cyber components, we assess the most occurring components of projects of innovators who perceive the importance of cybersecurity either as moderately high or extremely high (see Table C.4). This filter presents components which occur in systems where the cybersecurity of that system is highly rated. We do the same for projects with (very) satisfied innovators concerning the current cybersecurity efforts (Table C.5).

The perception of the innovators on the importance of cybersecurity and their satisfaction with the cybersecurity efforts in their project are involved in determining the cases for this study. We present the response to these questions in Figures C.5 and C.6. Figure C.3 compares the results from the two ratings. No dissatisfaction with the current cybersecurity efforts is reported. At the same time, we see a satisfaction increase with the increase in the perceived importance of cybersecurity. The innovators' valuation of importance for the cyber component categories is also surveyed (see Figure C.7). The data collection category is perceived as most important, followed by both the control and data processing categories. The average importance score for communication is just below these categories, whereas the physical components follow with a significantly lower perceived importance from the innovators. We also compared the importance of the categories divided by the cybersecurity importance (Figure C.8) and satisfaction with cybersecurity efforts (Figure C.9 answer options.

Table C.1: Code table of the survey

Question	Description	Variable	Code
1	Name of Project	name	selection from list
2	(Name when not on BRIGAIDs List)	name_other	open answer
3	Importance cybersecurity	cybersecurity_importance	0 = not applicable 1 = not at all important ... 5 = extremely important
4	Satisfaction with cybersecurity efforts	cybersecurity_satisfaction	0 = not applicable 1 = very dissatified ... 5 = very satisfied
5	Addition to categories	other_category	open answer
6	Communication through landline	communication_landline	0 = no, 1 = yes
7	Communication through mobile line	communication_mobile_line	0 = no, 1 = yes
8	Communication through satellite	communication_satellite	0 = no, 1 = yes
9	Human Machine Interface	communication_hmi	0 = no, 1 = yes
10	Other communication component	communication_other	0 = no, 1 = yes
11	(namely)	communication_other_component	open answer
12	Servers	control_servers	0 = no, 1 = yes
13	Firewall	control_firewall	0 = no, 1 = yes
14	Anti-virus	control_anti-virus	0 = no, 1 = yes
15	Feeder protection relays	control_feeder_relays	0 = no, 1 = yes
16	Malfunction Management Unit	control_mmu	0 = no, 1 = yes
17	Other control component	control_other	0 = no, 1 = yes
18	(namely)	control_other_component	open answer
19	Real-time data	collecting_real-time_data	0 = no, 1 = yes
20	Smart meters	collecting_smart_meters	0 = no, 1 = yes
21	Cameras	collecting_cameras	0 = no, 1 = yes
22	Other types of sensors	collecting_sensors_other	0 = no, 1 = yes
23	(namely)	collecting_sensors_other_component	open answer
24	Other data collecting component	collecting_other	0 = no, 1 = yes
25	(namely)	collecting_other_component	open answer
26	Cloud technologies	processing_cloud_technologies	0 = no, 1 = yes
27	Offline data storage	processing_offline_storage	0 = no, 1 = yes
28	User interface	processing_user_interface	0 = no, 1 = yes
29	Autonomous decision-making	processing_autonomous	0 = no, 1 = yes
30	Data processing/analysis tools	processing_data_analysis	0 = no, 1 = yes
31	Other types of actuators	processing_actuators_other	0 = no, 1 = yes
32	(namely)	processing_actuators_other_component	open answer
33	Other data processing component	processing_other	0 = no, 1 = yes
34	(namely)	processing_other_component	open answer
35	Accessible hardware (insiders)	physical_accessible_insiders	0 = no, 1 = yes
36	Accessible hardware (outsiders)	physical_accessible_outsiders	0 = no, 1 = yes
37	Network access points / Points of entry	physical_access_points	0 = no, 1 = yes
38	Environment	physical_environment	0 = no, 1 = yes
39	Other physical component	physical_other	0 = no, 1 = yes
40	(namely)	physical_other_component	open answer
41	Ranking importance of the categories	categories_ranking	most important (5) ... least important (1)
42	Remarks, recommendation, lessons	remarks	open answer
43	Contact information	contact	open answer

Algorithm C.1: Pseudo code of the R script

```
working directory is set to the R map in My Documents
load in the necessary libraries (data.table, plyr, ggplot2)
load in the export data from the survey. The file is formatted by SurveyGizmo
surveydata ¡- "SurveyExport.csv"
create dataframe results from the export, exclude columns that serve no purpose in this study
results = subset(surveydata, select = delete unused columns
rename the columns, since renaming all 44 columns at once produced an error, we split the
  function in four sub functions
setnames(results, old column names, new column names)
qual_results = subset of results containing the columns with open answers
the qualitative data is exported to csv for further review
write qual_results to csv and name it "qualitative_results.csv"
results = subset of results without the columns with open answers
recode the component values with 1 ( = component in project) and 0 ( = component not in
  project)
missing values are also treated as 0 ( = component not in project)
recode the two questions with Likert rating scales to 1-5 scale, with 0 value for "not applicable"
NOTE: This section is a manual action for cleaning wrongful data. Revise before running entire
  script
the first response was a test run, which is deleted from the results
results = results without the first row
Some respondents checked the 'other' components box, but gave an answer in the sense that
  this component does not apply to their project. This while that component is still counted as
  one for the total sum. We adjust this by manually changing these values from 1 to 0
results of rows 4,8,11 adjusted to 0 for other variables
We calculate the number of components per category
results total columns = sum of components within the categories
We now calculate the total number of components in a project
results total_componentscolumn = sum of all total columns
Data from the Climate Innovation Window on the Hazard, Topics, and TRL of projects is loaded
  in the script
webdata = dataframe with data from "webdata.csv"
set names of webdata columns to lower case names
We merge the data from the CIW with the results from the survey
df = dataframe with data from results and webdata dataframe, with the name column as pivot
haz = dataframe that counts the hazard data
t1,t2,t3 = dataframe that counts the topic data
tt = dataframe that merges t1,t2,t3
Most used components
components = subset of results dataframe with only the component columns
Data from the importance of categories
cats = dataframe with data from "category_score.csv"
Before visualization, we save the results dataframe as a csv file
write df to csv file named "results.csv"
VISUALIZATION
install ggplot2 package
plot of the frequency of hazards named "hazards.png"
plot of the frequency of topics named "topics.png"
prepare data: group sum of components by category
plot of the number of components per category
plot of the Importance vs Satisfaction of Cybersecurity named "importance_satisfaction.png"
scatterplot of the importance score on x-axis and satisfaction score on y-axis
chart of the ranking of importance for component categories named "importance_categories.png"
plot of the number of components per category
chart of the ranking of most counted components named "component_count.png"
plot of the number of components per category
```

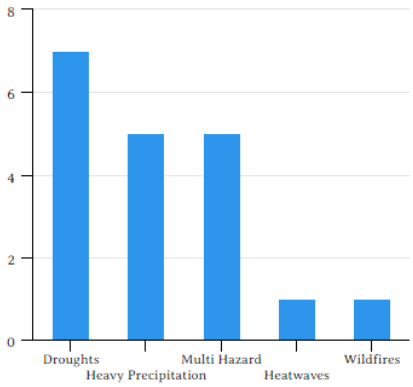


Figure C.1: Number of respondents per hazard

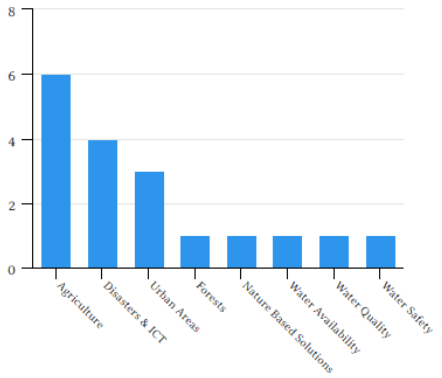


Figure C.2: Number of respondents per topic

Table C.2: Ten most occurring components

Component	Count
Data processing/analysis tool	13
Servers	12
Anti-virus	11
Accessible hardware (for insiders)	11
Human Machine Interface	10
User interface	9
Firewall	9
Communication through mobile line	8
Offline storage	8
Smart meters	7

Table C.3: Classification of newly added components from survey data

Other Component	Classification
Internet	Communication mobile line
GPRS	Communication mobile line
GPS Data	*added as component*
Mechanical component	*added as component*
Drones	*added as component*
Manually entered data	*added as component*
Simple data structure	Offline data storage
GIS	*added as component*

Table C.4: Components with high CS importance
Ten most occurring components in projects with high perceived importance of cybersecurity

Component	Count
Servers	7
Communication through mobile line	7
Offline storage	7
Data processing/analysis tool	6
User interface	6
Anti-virus	5
Firewall	5
Human Machine Interface	4
Real-time data	4
Accessible hardware (for outsiders)	4

Table C.5: Components with high satisfaction
Ten most occurring components in projects with high satisfaction with cybersecurity efforts

Component	Count
Servers	7
Communication through mobile line	6
Offline storage	5
Data processing/analysis tool	5
User interface	5
Anti-virus	4
Firewall	4
Human Machine Interface	4
Real-time data	4
Communication through landline	4

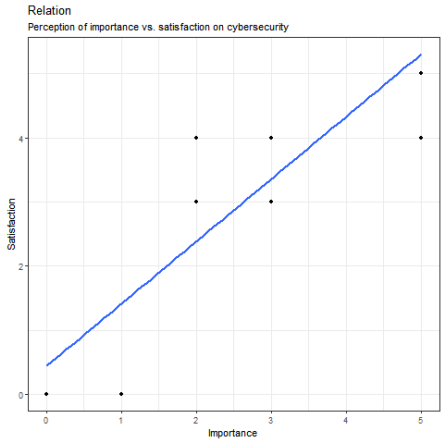


Figure C.3: Perception of cybersecurity importance vs. satisfaction with cybersecurity efforts

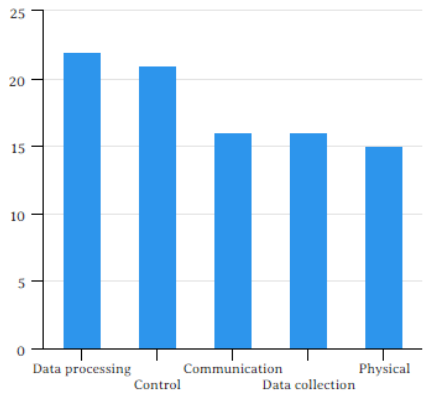


Figure C.4: Number of components per category

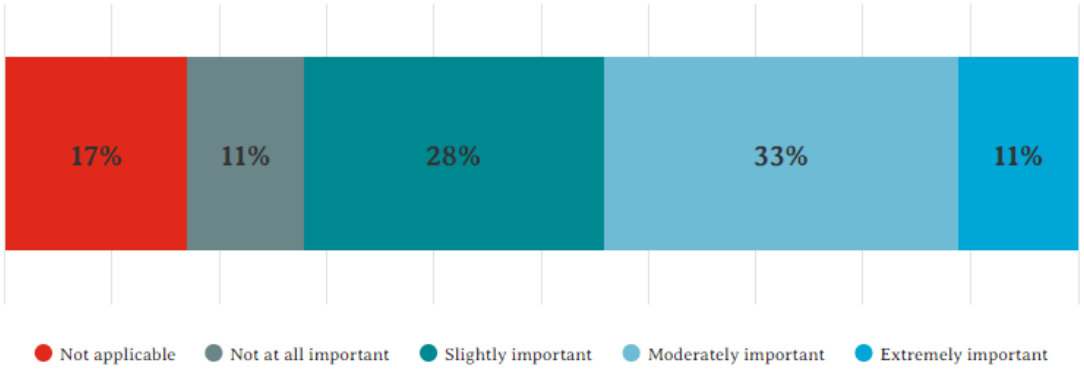


Figure C.5: Perceived Importance of Cyber Security

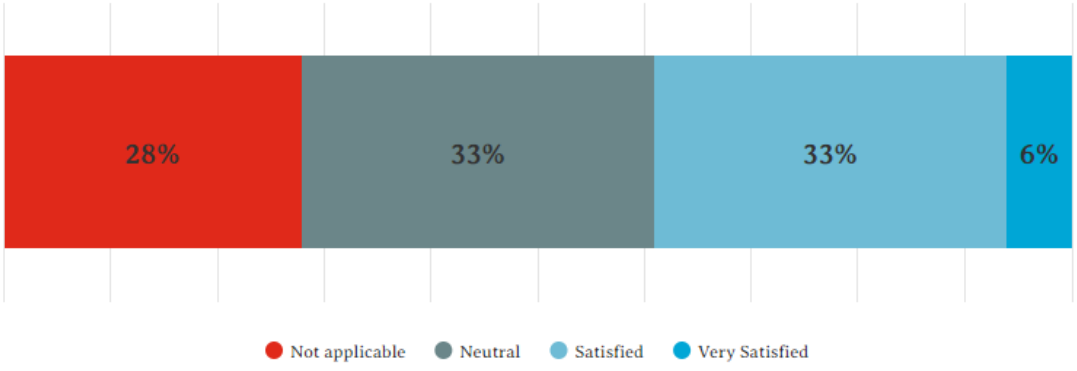


Figure C.6: Satisfaction with Cyber Security Efforts

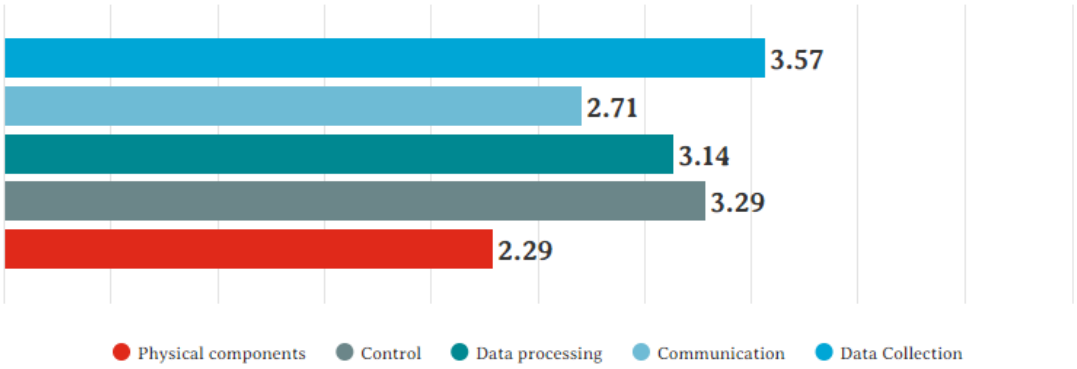


Figure C.7: Average Category Importance Score

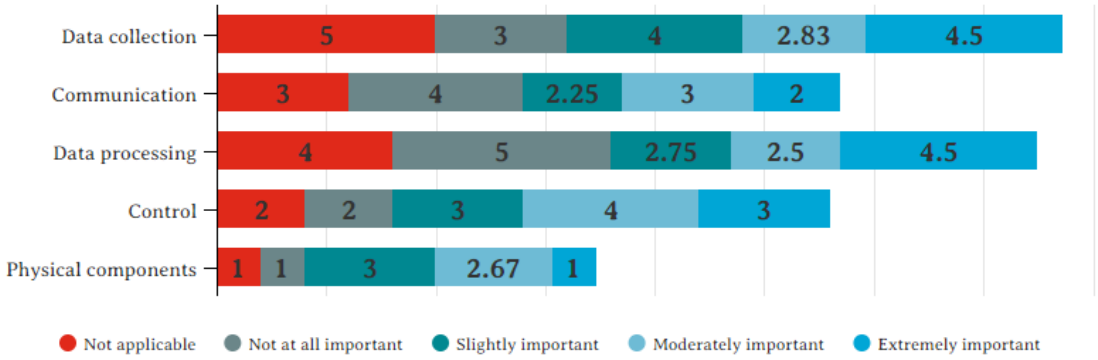


Figure C.8: Average Category Importance Score per Perception of Cyber Security Importance

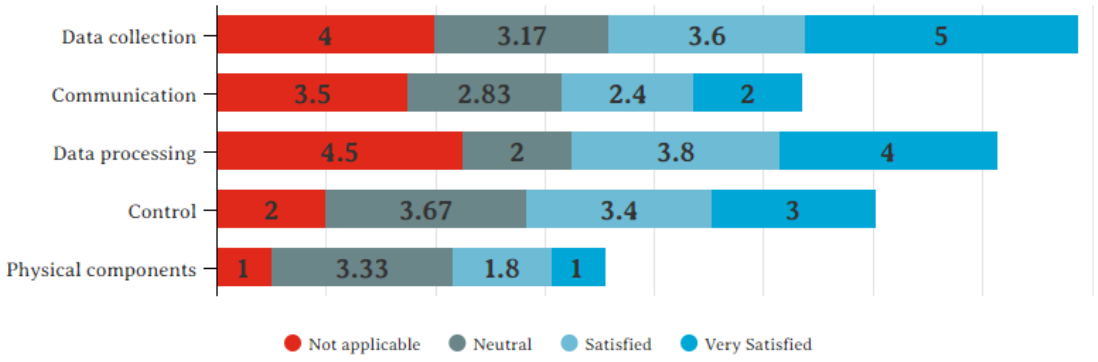


Figure C.9: Average Category Importance Score per Satisfaction with Cyber Security Efforts