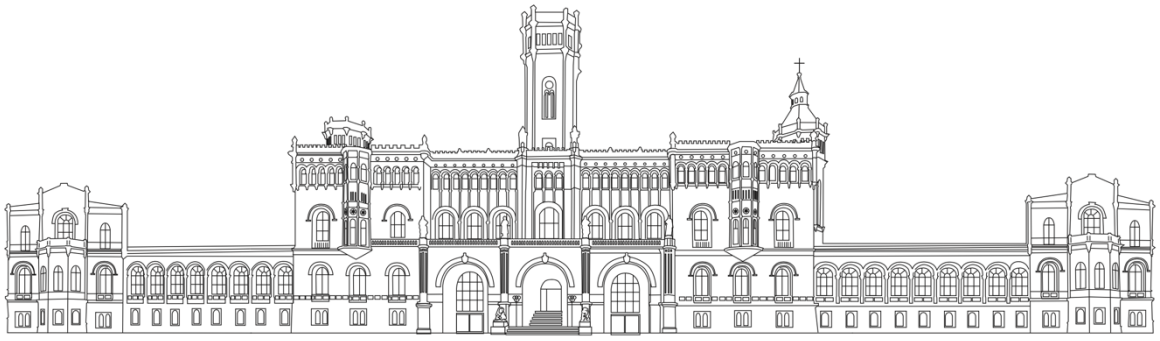

Gottfried Wilhelm Leibniz Universität Hannover
Institut für Wirtschaftsinformatik

Resilience for Future Energy Supply: A Taxonomy and Archetype Analysis of Cybersecurity Services

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B. Sc.)“ im Studiengang Wirtschaftsingenieur der Fakultät für Elektrotechnik und Informatik, Fakultät für Maschinenbau und der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von:

Name: Bertram Vorname: Johannes Ludwig
[redacted]

Prüfer: Prof. Dr. rer. nat. M. H. Breitner
Betreuerin: M. Sc. Jana Gerlach

Hannover, den 17.08.2022

Table of Contents

1 Introduction

This bachelor's thesis addresses the topic ' Resilience for Future Energy Supply: A Taxonomy and Archetype Analysis of Cybersecurity Services'.

Climate change reminds us of the need to replace our fossil fuel-based system of energy consumption with one based on renewable energies. The relevance of this bachelor's thesis is visualized using a six-step chart depicted in Figure 1.1. We have now reached step two. In the electrical energy supply sector, there is an increased demand for carbon dioxide-free energy generation for two reasons. First, due to the transformation of all sectors such as industry, transport and private households, away from the use of fossil energy to the use of electrical energy, there is a still increasing demand for electricity. Second, the way of energy generation needs to be changed to carbon dioxide free generation.

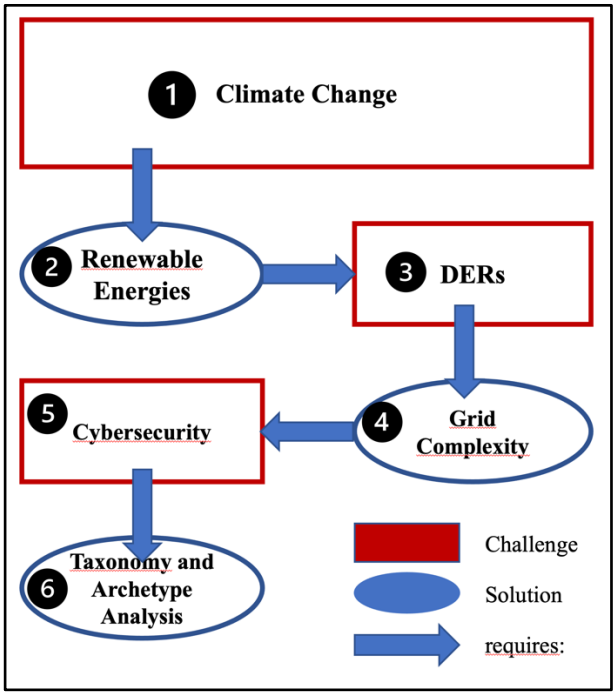

Figure 1.1: Visualization of relevance

The reduction of CO_2 emissions in power generation causes the need for the expansion of renewable energies. Renewable energy sources such as wind turbines or photovoltaics often appear in the type of Distributed Energy Resources (DERs), which brings us to step 3 of the diagram. The distributed nature of the placement of these DERs requires a complex design of the power grid. Because this complex grid requires many smart components, the vulnerability to cyberattacks on the power grid increases as well. To maintain resilience in power supply, approaches are needed to protect utilities with cybersecurity services. Because of the constantly growing number of cybersecurity services in the energy sector and the missing literature regarding an overview on this topic, the relevance of a research is identified. The type of research will be clarified by posing two Research Questions, which are presented below:

RQ1 What does a taxonomy of cybersecurity services for utilities look like?

RQ2 Which archetypes can be identified with the help of an archetype analysis based on the taxonomy of cybersecurity services for utilities?

To date, there is no literature that approaches the field using the scientific classification method of a taxonomy. Based on the research questions, a taxonomy of cybersecurity services in utilities is developed. On the basis of the taxonomy, archetypes are identified.
The thesis is structured as follows. In the second chapter, the motivation and relevance of the topic is discussed in the context of climate change. To avoid uncertainty about the above-mentioned terminology, the principles of energy supply and cybersecurity are explained in chapter 3. Chapter 4 presents the methodological approach of taxonomy development after Nickerson et al. (2013). The literature review according to Brocke et al. (2015) and Webster and Watson (2002) is also conducted in the chapter. The Final Taxonomy including six iterations is built in Chapter 5. Chapter 6 identifies four archetypes based on the taxonomy by applying a cluster analysis. Finally, the results of this bachelor thesis are discussed, limitations are indicated, and a conclusion is drawn.

10 Conclusion

In this Bachelor's theses the resilience of future electric energy supply was examined. First, the relevance of the matter was explained by reasoning the need to drastically reduce the emission of greenhouse gases. The extension of renewable energies in the power system and accompanying risks of cyber attacks were found out based on a literature review after Webster and Watson (2002). A taxonomy and archetype analysis of cybersecurity services was conducted to expand the literature with an empiric overview.
The methodology of the taxonomy development process after Nickerson et al. (2013) was described. Also, the first Research Question was addressed.

> RQ1 What does a taxonomy of cybersecurity services for utilities look like?

In the scope of this question a taxonomy of cybersecurity services with 6 iterations was performed. A final taxonomy with 9 dimensions and 31 characteristics is available. For the taxonomy, a list of 22 cybersecurity services for utilities was found using a Crunchbase search. The taxonomy's outcome and impact of limitations were interpreted and lead to an image of a market that primarily covers the areas overview, and detection of vulnerabilities and incidents. It is concluded that specialization, future technologies and human errors could still be a gap in the market. Also, the reasons for chosen characteristics of the taxonomy were discussed. The cause of questionable characteristics lies in biased information from the side of the provider.
Based on the taxonomy, an archetype analysis was performed according to the second Research Question.

> RQ2: Which archetypes can be identified with the help of an archetype analysis based on the taxonomy of cybersecurity services in utilities?

4 archetypes were identified and named according to key-characteristics. The archetypes are 'Interior vulnerabilities and human risk factor', 'Modern device protection and data analysis', 'Modern grid authentication and Public Key Infrastructure', and 'External threat warning and ICS protection'. The method of the archetype analysis was discussed, and alternatives were pointed out.
Afterwards, the demand for the taxonomy and archetype analysis was justified by speculation on potential attackers. Additionally, the evidence of three statistics was used stating that most utilities consider cyberattacks as a challenge of digitalization and many utilities have already become victims of attacks. For that reason, and the aspect of missing literature, it was concluded that the companies are interested in the taxonomy and archetype analysis. This way the work provides useful guidance, inspiration and innovation approaches for the design of services, and shows empirical frameworks that exist in the market. As an outlook, the possible creation of a classification tree with its use for researchers was pointed out.