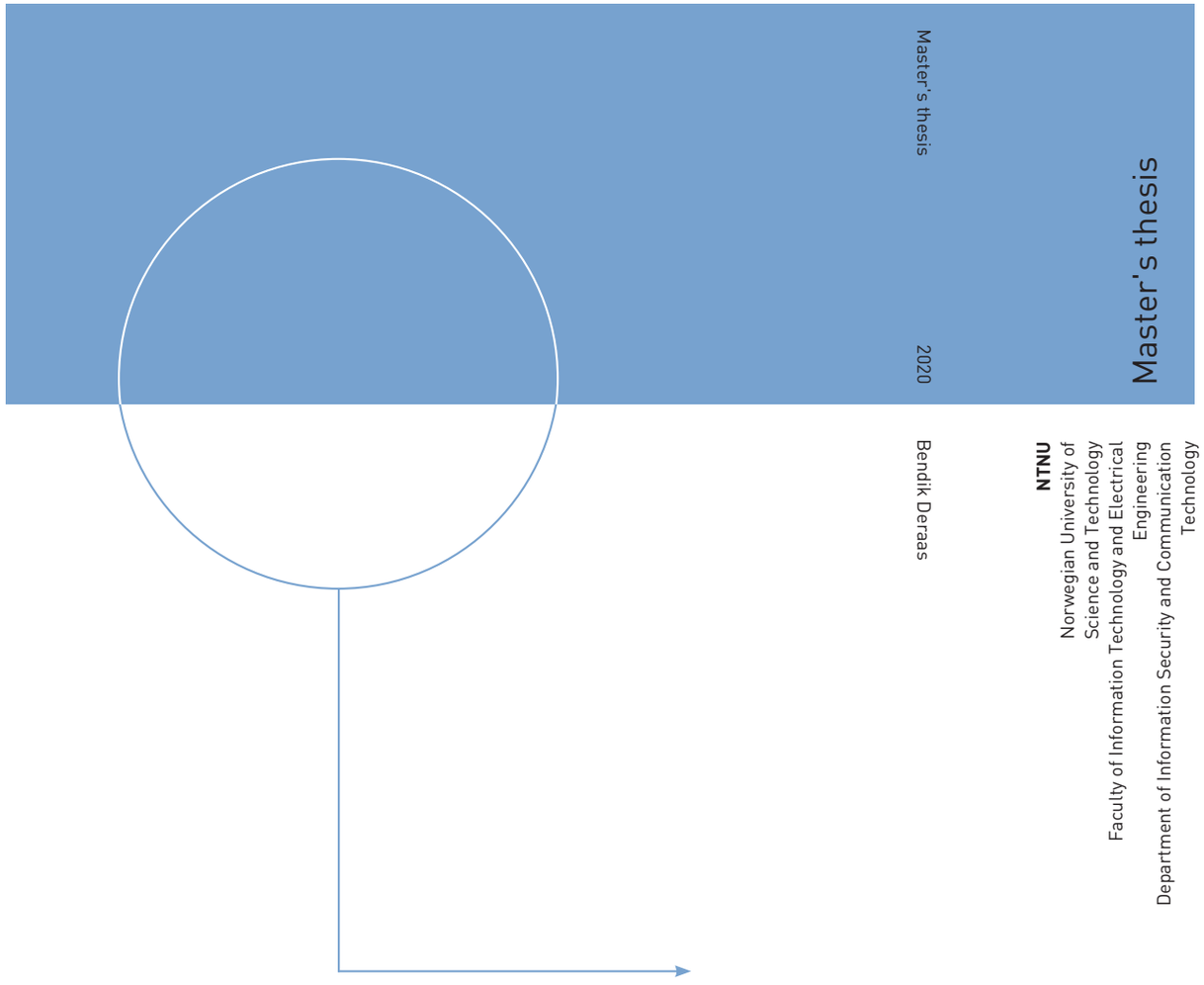

Master's thesis

2020

Bendik Deraas

NTNU
Norwegian University of
Science and Technology
Faculty of Information Technology and Electrical
Engineering
Department of Information Security and Communication
Technology

Bendik Deraas

Modelling and Analysis of Interdependencies between Financial, Communication and Power System Infrastructures in a Smart Grid Scenario

June 2020

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

NTNU

Norwegian University of
Science and Technology

Modelling and Analysis of Interdependencies between Financial, Communication and Power System Infrastructures in a Smart Grid Scenario

Bendik Deraas

Communication Technology
Submission date: June 2020
Supervisor: Bjarne E. Helvik
Co-supervisor: Michele Garau

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

Title: Modelling and Analysis of Interdependencies between Financial, Communication and Power System Infrastructures in a Smart Grid Scenario

Student: Bendik Balstad Deraas

Problem description:

The infrastructures that provide critical services to society are tightly interconnected. An internal perturbation on each of these infrastructures affect the connected infrastructures, with possible cascade effects that can lead to systemic blackouts. Evaluating the extent of the dependencies of an infrastructure to the interconnected infrastructures, and the possible vulnerabilities that such dependencies entail, represents a fundamental requirement for risk assessment. By modelling the infrastructures and their dependencies, interdependencies can be identified and understood. Identifying these interdependencies will give more accurate risk assessments, potentially cascading failures can be predicted, and in turn, this knowledge can be used to strengthen all the related infrastructures.

The financial infrastructure and its interdependencies have not been studied extensively, and the lack of research on this topic has been mentioned in several literary studies. Most of the financial services are becoming fully digital, increasing the dependence on other critical infrastructure. In parallel, the introduction of 5G in the communications infrastructure creates a shifting landscape for all online services. Power systems are also greatly affected by this shift, opening for the introduction of smart grid technology. By using financial transaction in a smart grid context as a case study to model the three different infrastructures, interdependencies can be identified and analysed to provide knowledge and insight into the 5G transition as well as the smart grid implementation.

The thesis work consists of the following tasks: - Research on vulnerabilities and interdependencies between infrastructures and comparative analysis of different modelling approaches in this context. - Development of a model for dependability assessment of the financial infrastructure in relation to the communication and power infrastructure. - Using the result from the model to identify interdependencies that can be used to create mitigation strategies against failures and cascading effects.

Date approved: 2020-02-14

Supervisor: Bjarne E. Helvik, Responsible professor

Cosupervisor: Michele Garau, Supervisor

Abstract

Society is becoming increasingly interconnected, and so is the infrastructures that support it. One of the most significant threats to infrastructure security is interdependencies developed between them. The increasing interconnections between infrastructures support them to become more reliable, efficient and robust. However, the consequent increase in interdependencies creates a complex network which can hide critical interdependencies for the functioning of infrastructure systems.

This thesis researches what interdependencies may develop between the financial, communications and power infrastructures in the migration towards a 5G and Smart Grid future. Previous works have failed to address financial infrastructure interdependencies in the technical domain. This thesis studies the technical structures present in the financial infrastructure, which is part of the foundation for this model. Studying the financial infrastructure in the context of 5G and Smart Grid developments will broaden the understanding of which interdependencies that may occur in the future.

By developing a model, we identify interdependencies between infrastructures. With the use of an agent-based approach, the model encapsulates the financial, communication and power system infrastructures on a subsystem level in a UML-diagram. From this model, we develop a java based simulator in the JADE platform. This simulator enables simulation of catastrophic failure scenarios to identify cascading failures inside and across the infrastructure systems.

The steady-state simulation shows how the market is an exposed and vulnerable entity in the infrastructure systems. Simulations of catastrophic failure in data centres shows how this causes a cascading failure that produces devastating recovery challenges for critical Smart Grid functionality. The simulation results prove how interconnected these infrastructure are, and how each subsystem is critical for the workings of another.

Sammendrag

Samfunnet blir stadig mer sammenkoblet, og det samme blir infrastrukturene som underbygger det. En av de viktigste truslene mot infrastruktursikkerhet er gjensidige avhengigheter som utvikles mellom dem. Den økende sammenkoblingen mellom infrastrukturer støtter de til å bli mer pålitelige, effektive og robuste. Imidlertid skaper en økning i avhengigeter et komplekst nettverk som kan skjule kritiske avhengigheter for infrastruktursystemenes funksjon.

Denne avhandlingen undersøker hvilke gjensidige avhengigheter som kan utvikle seg mellom finans-, kommunikasjons- og kraftsysteminfrastrukturen ved introduksjonen av 5G og Smart Grid teknologi i fremtiden. Tidligere arbeider har ikke adressert teknisk gjensidige avhengigheter i den finansiell infrastrukturen. Denne avhandlingen studerer de tekniske strukturer som er til stede i den økonomiske infrastrukturen, som danner grunnlaget for denne modellen. Ved å studere finansinfrastrukturen i sammenheng med utviklingen av 5G og Smart Grid vil vi utvide forståelsen av hvilke gjensidige avhengigheter som kan oppstå i fremtiden.

Ved bruk av en modell identifiserer vi gjensidig avhengighet mellom infrastruktur. Modellen er utviklet med en agentbasert tilnærming, og illustert ved å inkapsulere finans-, kommunikasjons- og kraftsysteminfrastrukturen på et systemnivå i et UML-diagram. Fra denne modellen er det utviklet en java-basert simulator i JADE-plattformen. Denne simulatoren muliggjør simulering av scenarier av katastrofale feil for å identifisere sammenfallende feil i og på tvers av infrastruktursystemene.

Stead-state-simuleringen viser hvordan markedet er en eksponert og sårbar enhet i infrastruktursystemet. Simulering av katastrofale feil i datasentre viser hvordan feilen propagerer og skaper store utfordringer ved gjennopprettelse av kritisk Smart Grid-funksjonalitet. Simuleringsresultatene viser hvor tett infrastrukturene er koblet sammen, og hvordan hvert delsystem er kritisk for en annen.

Preface

This master thesis was written spring of 2020 at the NTNU – Norwegian University of Science and Technology's Department of Information Security and Communication Technology. Responsible professor Bjarne Helvik composed the framework for this master thesis problem description. Proposing a general aim at modelling interdependencies in critical infrastructure, I provided interest and knowledge in the financial infrastructure from previous internships in DNB. Discovering the lack of research around modelling interdependencies in the financial infrastructure combined with the exciting changes implicated by the 5G shift, created an opportunity for exploring new ground. I have found that studying the modelling of interdependencies and its implications for infrastructure security is compelling. This thesis has been a challenging and exciting project, but I hope to encounter this field of research in my future endeavours.

I want to thank my supervisors Bjarne Helvik and Michele Garau, for providing steady guidance in this complex field. Their reliable feedback and support has motivated my work and been a valuable contribution to this thesis. I want to direct a huge thanks to my parents Kari and Ståle for their unwavering support. Much of my curiosity, perspective, and knowledge is owed to their hard work and patience throughout the years. I would also like to thank Madeleine for the motivating and supportive discussions we have had the past months.

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Infrastructures are the systems comprised of facilities, services, and installations that serve as an underlying foundation for society. Technological advances evolve infrastructures to become increasingly interconnected. This increase in interconnection creates opportunities and may stimulate new developments across industries. However, this increase also creates more dependencies and interdependencies across infrastructures. One of the significant threats to infrastructure functionality is cascading failures as a consequence of unidentified interdependence. This thesis explores how infrastructure interdependencies can be identified and analysed through modelling.

1.1 Background

The introduction of 5G technology proposes a radical shift in the communication infrastructure. This shift enables massive changes in the infrastructures setting requirements for the communication infrastructure. One of the emerging changes to the power infrastructure is Smart Grid technology. This technology allows for decentralised production of electricity and planned consumption which is predicted to stabilise the increasing demand on the power grid.

The implications of the 5G shift for the financial infrastructure is more uncertain than for the power infrastructure. However, the shift will enable higher data speeds and capacity for customers and lower the cost of operating ICT-services for the bank. In turn, this will make the 5G a catalyst for banks to stay better connected with their customers. The 5G shift sparks innovation with broad implication for the power markets, following the decentralisation aspect of the Smart Grid development, the markets might follow.

Interdependence is one of the main challenges for infrastructure security and should be addressed in the development of reliable and resilient infrastructure. The overall trend in technology is that everything is becoming more interconnected, and

this includes infrastructures. The 5G shift will contribute to this in a significant way. With lower latency and higher capacities in data transfers, systems can communicate and become more efficient, but in the process, they become more interconnected. All these interconnections ultimately create interdependencies that threaten the reliability of the entire infrastructure system.

1.1.1 Initial Case

These technological advances create motivation in the form of an initial case for this thesis. The Smart Grid technology enables each household to become producers and consumers of electricity, and this requires functioning platforms and the ability to plan and trade electricity. For a Smart Grid household to function properly, it sets requirements for three different infrastructures:

- The financial infrastructure is required to provide platforms of trade and enable monetary transactions for the trading of electricity for the household Smart Grid actor
- The communication infrastructure is required to provide connectivity and service for the operation of the Smart Grid, as well as supporting the financial infrastructure
- The power infrastructure is required to provide the operational functioning of the households Smart Grid

This initial case sets the scope of the model. The proceeding chapters aims to understand the technical aspects of the infrastructures ability to meet the requirements of this initial case.

1.2 Contribution

The overall goal of this master thesis is to provide knowledge and information about the communication infrastructures interdependencies with the financial and power system infrastructures. As society and technology are becoming more complex, the need for clarity and understanding is also increasing. Modelling infrastructures enables a better understanding of these complex systems, and assists in creating cases and predictions to further strengthen the systems.

The 5G shift proposes massive developments in all infrastructure that serves critical functions for society. By simulating the predicted implementation of 5G technology, interdependencies can be identified. Analysing the interdependencies identified in this thesis will assist in mitigating risks of cascading failure, which can ensure effective measures to increase infrastructure robustness.

Reviewing the state of the art research and literature review on the topic of infrastructure interdependency modelling, it is clear that the financial infrastructure interdependencies lack research from a technical standpoint. This thesis will provide a new piece of technical understanding by connecting the financial infrastructure with the communication and power infrastructure and identifying their interdependence and common dependencies.

This thesis also provides an analysis and review of different modelling approaches and tools for the modelling of three infrastructures in this given context. Studies with the scope of more than two infrastructures are often large mappings or reviews with little detail in regards to the required functionality of the infrastructures. The lack of such models creates uncharted territory for the development of models with the scope of three infrastructures, including a level of detail that is more nuanced than the total output of the infrastructures.

The thesis describes the process of providing a model to identify interdependencies between the financial infrastructure, 5G communications infrastructure, and the Smart Grid power infrastructure. This modelling is based on the initial case, which serves as a representation of a near-future scenario, and illustrates the complexity that will develop with the current technological advancements.

1.3 Thesis Outline

Chapter 2 gives the reader a theoretical background to understand the field of infrastructure interdependencies. Further, Chapter 2 presents background into the different infrastructure systems that provide functions to the initial case requirements. From this background, the objectives and research question of this thesis is developed and presented in Section 2.5.

Chapter 3 presents the method used to answer the research question, and consequently, the objectives along with an analysis of modelling approaches and tools. In Chapter 4, the model is described in the development stages of design and implementation. From this model, a simulator is developed to study the model behaviour over time. The results produced by the simulator is presented and discussed in Chapter 5.

The challenges of designing and implementing the model are discussed in Chapter 6 along with an evaluation of the model's representativeness and results. The thesis project is concluded in Chapter 7, after which Chapter 8 suggest future work.

Chapter 2
Theoretical Background and Infrastructure Study

The three critical infrastructures of finance, communications and power are currently in periods of transition. These transitions will have an enormous consequence for their surrounding infrastructures, including each other. Most notably, the communication infrastructure is continuing its development towards a more wireless future society. With the Internet of Things (IoT), Smart Grids, and an ever-increasing demand for higher performance and capacity in the wireless mobile networks, the communications infrastructure is racing to meet this demand with the introduction of the 5G network.

This chapter contains a summary of the theoretical background that assist in understanding the study of infrastructure interdependence and modelling. Further, this chapter lays the groundwork for an infrastructure interdependency model by presenting a study of the general functioning of the infrastructures and how the infrastructures meet the requirements presented by the initial case in Chapter 1. The infrastructure study also lays the foundation for the discussion and choice of the modelling approach, which supplies the framework for the model design and implementation.

2.1 Terms and Concepts in Infrastructure Interdependency Modelling

This section presents central concepts of interdependence modelling defined by state of the art research. These terms and concepts are used to understand events and results from the model and discussion.

2.1.1 Interdependence

Rinaldi defines *interdependency* as the bidirectional relationship between two infrastructures through which the state of each infrastructure influences or is correlated to the state of the other [51]. More generally, two infrastructures are interdependent when each is dependant on each other. *Interdependencies* describe connections among

agents in different infrastructures in an overall system of systems. In the real world, it is observed that interdependencies among infrastructures increase the overall complexity of the system of systems [51]. The risk from interdependency failure is challenging to calculate since some interdependencies can be almost invisible in normal operations, but when failure strikes, they emerge and become apparent.

Interdependencies are often described by types and scholars have developed several different sets of types and classifications, as summarised by Ouyangs review [46]. The different types of dependencies are important for describing the scope and limits of the model. To use the types defined in the most cited and acknowledged paper within the field of infrastructure dependency, we again look to Rinaldis 2001 paper [51]. By using the four different types of interdependency types as defined by in the Table 2.1 to describe the infrastructures interdependency, it can also help in limiting the modelling scope by focusing on one type. In this modelling, the cyber interdependencies are in focus, but both logical and physical interdependency types provide essential context.

Table 2.1: Interdependency types as defined by Rinaldi [51]

Interdependency Type	**Definition**
Physical	The state of one infrastructure system is dependent on the material output(s) of another infrastructure system
Cyber	The state of one infrastructure system depends on information transmitted through the information infrastructure
Geographic	A local environmental event can create state changes in two or more infrastructure systems
Logical	The state of one infrastructure system depends on the state of others via a mechanism that is not a physical, cyber, or geographic

The physical type of interdependence forms a basis for the functioning of all systems. Electrical power is produced and consumed, thus creating a dependence. This type can be applied for all infrastructures but is not the focus in this modelling.

Geographic interdependencies are becoming decreasingly relevant to the increase of connectivity, but this poses new challenges. As an example, most computing and data storage are no longer geographically dependant with their human operators and developers due to the evolution of cloud storage and computing. Moving data and processing to «off-site»locations which again are mirrored at different geographical locations, decreases the impact a local environmental event can have on the operation of infrastructure systems in the particular domains of finance, communication and power. Local events still have a massive impact, and geographic interdependencies

are essential to identify, but this identification has to be done on a more detailed level than this model proposes.

The logical interdependency type is somewhat of a leftover bucket and is easy to apply, but hard to analyse. Especially in the study of financial infrastructure, it is crucial to have such a type since the financial systems primarily consist of abstract mechanisms like trust, politics and market dynamics. These mechanisms have a massive consequence for the functioning of the infrastructures but are nearly impossible to predict and model. In the analysis section of the thesis, some of the logical interdependencies will be addressed, but including them directly in a technical model is difficult.

The cyber interdependencies are of the highest relevance in this modelling due to the cyber nature of the communication infrastructure which ties everything together. In the year of defining these types (2001), computerisation and automation of infrastructure systems were relatively new, but their definition still fit the current state of the infrastructures. As processing power and internet connectivity have increased dramatically, so has the infrastructure systems dependency on them. By focusing on the cyber and logical types, the model is limited and able to look beyond the electric power from the power infrastructure, which may cloud the results.

2.1.2 Failure Types

Along with different types of interdependencies, there are different types of failures. Failure is a disruption or an outage of a system, which can be caused by multiple factors. Rinaldi classifies the different failures as *cascading*, *escalating*, or *common cause*. By classifying the different types of failure, we can efficiently describe the level of severity and the confinements of the failure from a single infrastructure to the propagation of failures in several infrastructures.

Failures are the leading cause of interdependencies being a risk for infrastructures. Using the defined failure types in Table 2.2 allows us to describe better the threat faced by interdependencies, this again assists in the mitigation work against these threats.

2.1.3 Reliability

Reliability is a probabilistic measure of elements in an infrastructure system and their ability not to fail or malfunction. Reliability refers to the probability that an element in the system is functional. In contrast to the reliability, vulnerability is a broader concept with wider implications. While reliability focuses on the possibility of maintaining the performance of critical infrastructure elements, vulnerability focuses

Table 2.2: Failure types as classified by Rinaldi [51]

Failure Type	**Definition**
Common cause	occurs when two or more infrastructure networks are disrupted at the same time: components within each network fail because of some common cause
Escalating	occurs when an existing disruption in one infrastructure exacerbates an independent disruption of a second infrastructure, generally in the form of increasing the severity of the time for recovery or restoration of the second failure.
Cascading	occurs when a disruption in one infrastructure causes the failure of a component in a second infrastructure, which subsequently disrupts the second infrastructure.

on the potential for disrupting these elements or degrading them to a point where performance is diminished. This is a subtle yet essential difference [42].

Failure rate and failure probability concepts are introduced to describe and evaluate the reliability and vulnerability of the components. The failure rate represents the frequency in which a component in the infrastructure fails or malfunctions expressed in failures per unit of time. The failure probability, however, represents the probability function that a component will fail.

Reliability engineering is critical for planning and operating infrastructure systems, and it frames a wide field of research. The scope of this thesis is however limited to identifying interdependencies, and while implementing failure probabilities increases the accuracy of the model, it demands far greater insight and estimations of component behaviour than is appropriate for this project. This project will operate on estimated failure rates of components, and discuss the implications this has for the reliability and vulnerability of the infrastructure systems as a whole.

Summarised:

- If a component is highly reliable, it works for a long time without failure.
- A component with high availability does not fail often, and when it does, it can quickly be restored.
- The failure rate addresses the frequency at which a component fails.

2.1.4 Modelling and Simulation

There are necessarily two directions to go in investigating interdependencies in infrastructure:

- Knowledge-based approach: Conducting extensive qualitative empirical investigation of previous events
- Model-based approach: Developing an representation (model) of the infrastructures and its behaviours

The knowledge-based approach is an extensive qualitative approach and focuses on empirical investigation, expert interviews, and analysis of previous events. By researching data from events of system failure (as Rahman has done for infrastructure, with public failure reports [49]) the scope and consequence of infrastructure failure can be identified. Using the knowledge-based approach can provide critical qualitative assessments of severity in a relatively short time frame for decision-makers. However, due to its empirical nature, the results accuracy is dependant on the quality and interpretation of the acquired information. Seeing as both Smart Grid and 5G communication is in the early stages of development, there is not enough empirical knowledge or critical events to analyse in order to obtain accurate and appropriate information for mitigation. For developing the knowledge with appropriate accuracy to predict critical failure events and cascading failures, a model-based approach is considered more appropriate.

The concept of modelling refers to the development of a representation of a system. This representation aims at understanding and explaining complex concepts or systems. Models can represent physical objects or abstract concepts, and everything in between. A model is considered an abstraction to a varying degree, that implies an element of simplification in the model. It is said that a model is never perfect since its purpose is to simplify as well as describe accurately. Finding a balance between simplification and accuracy is the ultimate challenge in all modelling. Depending on the standpoint, something is always left out. The models level of abstraction compared to the real-world system is essential to understand in order to assess the models precision and set expectations of what is achievable with the model.

As society has become more digitised, the possibilities of modelling have increased. It is possible to model more extensive and more complex systems in various ways. Roads can be digitally modelled, and by running traffic simulations on these models, it is possible to predict events and consequences before they occur in real life. However, the field of modelling interdependencies in critical infrastructure is still relatively new. Due to the Y2K bug in late 1990, many realised how threatening

cyber interdependencies in the critical infrastructure are. Since then, the field has matured, and we see several modelling approaches are developed to identify interdependencies [51].

A principal challenge with the modelling of infrastructure is the sheer volume of data and knowledge needed to understand and model one infrastructure. It is therefore unusual to develop a model of more than two infrastructures with insight into the infrastructures inner workings [50]. Introduced in Chapter 1, the future will consist of more interdependence between several infrastructures, which drives research to explore the possibilities of interdependency modelling with broader scopes. In the following sections, the three infrastructures essential to the initial case are explored to create a basis for a model.

2.2 The Communication Infrastructure and the 5G Shift

Since the invention of the phone in the 19th century, the world has become an ever-smaller place, mainly because of the increase in communication capability. It is now possible to communicate all around the world, with both people and machines. This development must have been unimaginable 100 years ago. Nevertheless, a vast infrastructure has been developed to enable the sharing of information on an exponential scale. Looking at the development of communication technology, it is apparent that the future is wireless. The invention of mobile communication has made both information and knowledge widely available and has been one of the defining technologies of today's society.

Since the connection between the internet and cellular communication was made with the introduction of 2G technology, communication infrastructure development has been centred around wireless and mobile communication being an integrated part of the internet. The 5G shift is the latest in mobile technology and has the goal of creating a totally packet-switched mobile network. This shift includes a considerable amount of changes to the current infrastructure, and the final consequences of the implementation of 5G technology are partly unknown. The uncertainty of such a colossal shift makes it essential to research and investigate the potential scenarios that will arise with such a change. This investigation is done by creating models and simulating situations to discover events and cascading events that are hard to predict otherwise.

Creating a model of a technology still in development poses apparent challenges, and forces the use of assumptions and generalisation to tackle uncertainty. This section introduces background on the 5G development, based on literature studies of state of the art research on 5G, as well as white papers from different organisations responsible for the 5G development.

To better understand the impact of the 5G shift on the current infrastructure system, it is possible to utilise measurements and observation from the established 4G network and by taking target 5G performance figures into account, extrapolate its statistics to a 5G scenario. This approach is used by Bartelt to develop guidelines on designing 5G transport networks, and assists in modelling the 5G infrastructure [9].

By reviewing the design plan for 5G in the NGMN white paper, it is apparent that there will be significant implications for many critical societal functions [20]. The 5G provides an increase in both data transfer capacity, reliability and speed. Along with these upgrades, there are several new services included in the 5G. Many of these services will become essential to the development and integration of Smart Grid in society.

2.2.1 5G Architecture and Modelling Challenges

The proposed architecture of the 5G is complex and is composed of a large number of both physical and virtual components. By referring to the 5G architecture in this context, the network architecture is in focus. However, the network architecture has become a complex cyber-physical system. In Agiwals comprehensive literature study on the different suggested solutions for the 5G architecture, it is reasonable to state that the number of solutions highlights the challenge of uncertainty in this field [3]. The 5G is a technology evolved from the 4G/LTE technology, and although the 5G introduces several significant architectural changes, many of these changes are not definitive. It is, therefore, appropriate to describe 4G/LTE functions in places where there is significant uncertainty around how the 5G functionality and architecture.

The use of several modelling views is necessary for modelling and understanding the complex 5G architecture. In the 5G context, these views can be referred to as network slices, and are important in understanding the proposed functionality of the 5G architecture. Scholars have developed different version of network slicing to explain the 5G architecture [6, 52, 56]. Figure 2.1 provides a generalised and collective representation of the 5G architecture and splits the architecture into three network slices with one controller. The service layer, network function layer, infrastructure layer, and network slice controller all play different roles and depend on each other for providing the expected user experience.

In Figure 2.1, the focus for this infrastructure modelling will be the 5G infrastructure layer. This layer provides the infrastructure foundation of 5G network and is, therefore, the most crucial to explore first in such a model where the reliability of the infrastructure is concerned. As seen in Figure 2.1, the core network is a critical part of the network architecture of the 5G.

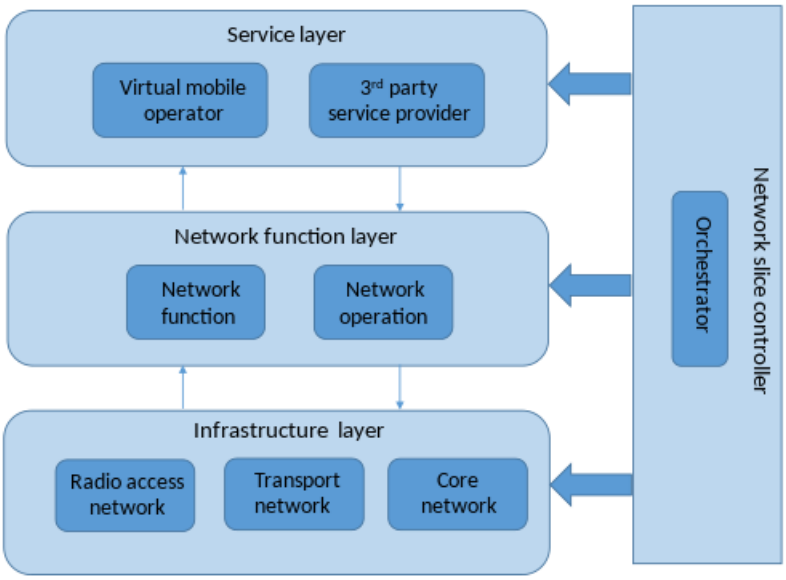

Figure 2.1: General architectural overview of the network slice [62]

Core Network

A stable core network is the heart of the communication infrastructure. The core network in the communication infrastructure consists of cables and routers that make up the backbone of the internet. In the shift towards 5G, mobile communication will depend on this backbone along with the 5G Core Network(5GCN). Referring to the 5GCN may be ambiguous since there are many views, levels and representations referring to the 5GCN with different scope and functionality in mind.

The 5GCN is responsible for providing management and control of the 5G network. The 5GCN also functions as the routing point of the 5G users' data to and from the internet. By connecting to the transport haul, where data is transferred from the users, the 5G core network routes packets to the intended service. Along with the routing functionality, the core also has several important sub-functions which are responsible for providing essential functionality to the network and mobility aspect of the 5G architecture. These sub-functions can be found in more detail in Appendix A.2 [24]. In addition to these network functionalities, the 5G core is responsible for access to services hosted in the data centre.

Transport Network

The transport network of the 5G architecture is responsible for providing a connection to the user's mobile units. It is challenging to find a technical consensus on the optimal transport network architecture solution. Since there exist several proposed solutions to this part of the 5G network, a generalised model is used as a basis. By using a perspective from the mature 4G technology, the transport network is split into three components: the eNBs, the RAN, and the S-GW.

The start point of the 5G is considered to be the eNB, which is commonly referred to as base stations. The development from the previous generation of mobile networks is that the physical area covered by each eNB in the 5G is smaller, requiring a higher number of eNBs. This development allows for the implementation of new wireless radio technology which provides lower latency, higher data rates, and more reliability.

There are several suggested solutions for the intermediate steps between the eNBs and the 5GCN. Several of these solutions involve a Cloud Radio Access Network (C-RAN), and several of the C-RAN solutions are review in Checko 2014 paper [15]. Checko also performs a comprehensive review of advanced technologies that may be used in the 5G transport network. The uncertainty created by the number of suggestions for this part of the architecture is overcome by looking at the 4G solutions for a more certain model [23].

Figure 2.2 illustrates a compromised solution interpreted from the proposed migration(from LTE to 5G) solution by Ericsson [24]. The use of a Radio Access Network(RAN) component as a common access point for several eNBs located in a specific geographical area, for example, a municipality. This RAN component forwards data to a Service Gateway (S-GW) and further on to the Packet Gateway (P-GW). Several solutions suggest that both the S-GW and P-GW functionality will become virtual and merged into the 5GCN in future developments.

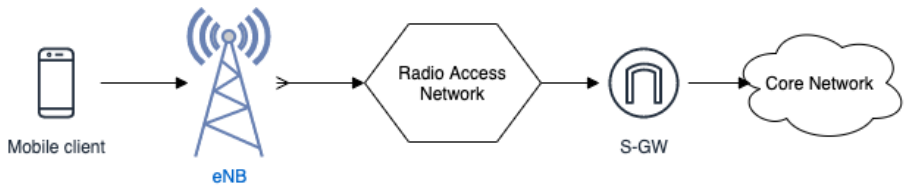

Figure 2.2: An simple illustration of the 5G transport network and the data packets road from the mobile unit to the Core Network.

2.2.2 5G service Supported by Edge and Cloud Computing

Along with increased network capabilities and reliability, the new element in the 5G shift is the introduction of services as part of the data network. In several papers, use cases are proposed as a way to define requirements of the future 5G service, and several applications of the new 5G service are exemplified [38, 20]. Among these cases are both services within the financial infrastructure and Smart Grid.

By increasing the data rates and reliability, the 5G increases the potential for data processing to be executed outside the mobile unit. Since increasing processing power in mobile units is increasingly difficult, the move to cloud computing can increase mobile unit applications available computing power to become relatively unlimited. Cloud computing in the 5G is split into two sections, the central processing and the edge processing.

There are several services proposed to meet the requirements for the 5G, set in the use cases developed by the 3GPP. For the case of Smart Grid and financial transaction, Mobile cloud computing (MCC), Multi-access Edge Computing (MEC), Ultra-reliable low-latency communication(URLLC) may be counted as the most essential. The URLLC service is provided by the new radio access technology which promises to provide high reliability and low latency communication for mobile units connected to the 5G.

MEC and MCC are the proposed services that advocate for more centralised processing of data. Mobile Cloud Computing can be considered a mature concept, as it involves processing done by centralised data centres instead of on computing units local to the user. The 5G is expected to increase the use of MCC, and with higher reliability and lower latency, it is predicted that several critical services will depend on MCC in the future.

A more drastic concept introduced by the 5G is the MEC, which makes use of processing and storage capabilities close to the air interface (eNBs) in order to deploy optimised services with minimum delay [25]. Instead of depending on centralised data centres like the MCC, the MEC concept proposes to shift data processing to the network edge, as an intricate part of the RAN. Establishing more processing power closer to the users enables operators to host larger applications and process content faster [33].

For the established MCC service, data centres are an essential part of the 5G architecture. Since most of the 5G core network functions will exist in a cloud-based environment, the data centres housing this functionality will be of critical importance to the physical security of the 5G. MCC facilitates the physical hosting of virtual services for several different critical societal function (as exemplified in [20])

which may create geographic interdependencies between infrastructures that have no intrinsic connection. As stated by Ahmad, this migration towards cloud computing creates several security vulnerabilities [4]. Considering that the MEC services are predicted to depend on computing capabilities in the edge network, there is reason to believe that the security that can be offered to the edge hosts is low in comparison to the centralised data centres hosting the MCC service.

2.3 Power System Infrastructure

Most countries rank the power system infrastructure as the most critical infrastructure, and with good reason. Developed societies are entirely dependent on power systems, mainly due to all other critical infrastructures dependency on power to function. Another factor that makes the power infrastructure highly critical is dependencies urgency. Even though health infrastructures have reserves and back-up power systems; there is reason to believe that a power outage of days would result in a high number of casualties [64]. There is much research to be found around the interdependence in power system infrastructure, and as Coerra finds in the 2013 paper on risk mapping the threats to this infrastructure type, functionalities from both financial and communications infrastructure are critical for the functioning of the power infrastructure [16]. Most cases involving Assets and financing risk, as Coerra describes it, do not rank as a critical threat to the current centralised architecture of the infrastructure. However, were this architecture to become more distributed this category of risk may become very different.

2.3.1 Central Power Systems

Power systems depend on power grids to distribute electricity to consumers. In automating and improving operations and functionality, the power grids depend on a Supervisory Control and Data Acquisition (SCADA) system. However, the dependence of the system has created cyber interdependence between power and communication infrastructure [13].

Traditional power systems infrastructure consists of centralised production and control. In an international context, the traditional power production plants are often fossil fuel plants like coal and gas plants. The traditional plants provide a steady energy source and have a low degree of failure and fluctuations in their production capacity. However, the world has increasingly become aware of the harmful sides of using fossil fuels, and the environmental impact this way of power production has. This awareness has fuelled a movement for a shift to renewable energy sources like wind and solar power.

With the demand for more electricity increasing, as well as a demand for more renewable energy, Smart Grid technology has been developed to address these demands. The Smart Grid aims at reducing the load on the transportation and distribution grids by local energy production and planning. This technology is enabled by the development of more reliable wireless communication, as well as technology enabling households to store and produce energy.

2.3.2 Smart Grid

In recent years the expansion of wind and solar power production has become significant, even though these sources have a weakness in its fluxing capacity, due to the uncontrollable nature of the weather. However, this weakness is possible to mitigate by planned smart consumption along with decentralised production. This capability is enabled by the Smart Grid technology, which is an emerging technology that allows for a household to become producers as well as consumers of electric power by developing a bidirectional power grid with improved control and monitoring of grid activity. The Smart Grid will also enable households to use electric cars and home batteries as storage units for electricity which can be sold depending on the demand that increases prices in the market. As the initial case in Section 1.1.1 proposes, the households in the Smart Grid will be more dependant on markets and financial transactions for the selling and buying of electricity, which again will directly influence the production and consumption.

The introduction of Smart Grid technology proposes a fundamental change to the power systems infrastructure, and implies a more distributed architecture, pushing for an evolution in the SCADA systems. Smart Grid technology implies more renewable energy sources, which proposes a challenge with intermittent power to the grid and in turn, stricter grid control to ensure stability in the grid.

Figure 2.3 captures a model of the Smart Grid infrastructure concerning the 5G network done by Cosovic where the 5G entities used by the Smart Grid are identified bottom-up [18].

In the modelling of the power infrastructure's logical and cyber interdependencies, it is essential to identify how the infrastructure is controlled. A critical functionality in the management and control of the electrical power systems is state estimation (SE).

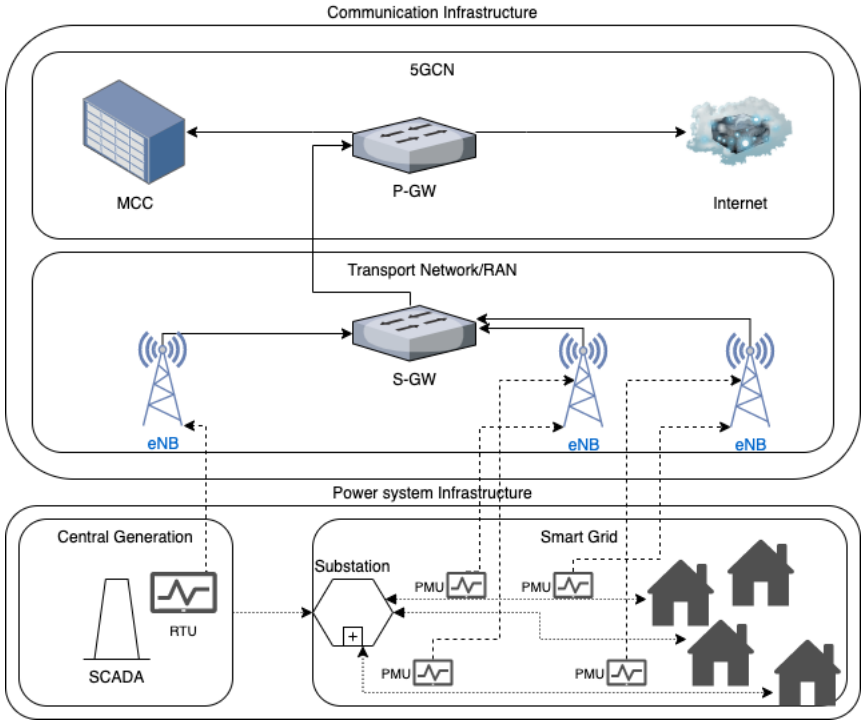

Figure 2.3: The architecture with two layers: i) power system infrastructure and ii) communication infrastructure that combines novel RAN interfaces supporting URLLC, and new virtualised core network (5GCN) MCC-based architecture with state estimation algorithm (SE) dependant on PMU and RTU measurement devices, to support future Smart Grid services such as distributed SE.

2.3.3 State Estimation

The goal of SE is to predict and describe the state of the power systems. It is strongly suggested that the emerging energy markets demand more reliable and accurate models for control and operation of the grid. The required accuracy can only be acquired by state estimators with reliable connections and data acquisition from measuring devices [8].

SE is currently being done in a centralised fashion, but according to Cosovic, this may not be applicable in the Smart Grid scenario due to the decentralisation and dynamic power grid evolution driven by Smart Grids [18]. Cosovic focuses on the implementation of phasor measurement units (PMUs) to accurately measure voltage and current phasors at high sampling rates. The use of PMUs, concurrently with the already implemented remote terminal units(RTU)(legacy) requires a wide area monitoring system (WAMS).

The WAMS would aim to detect and counteract power grid disturbance in real-time, requiring communication infrastructure to, ultimately providing the SE functionality:

- Integrate PMU devices with extreme reliability and ultra-low (millisecond) latency
- Provide support for distributed and real-time computation architecture for future SE algorithms
- Provide backward compatibility to legacy measurements traditionally collected by supervisory control and data acquisition (SCADA) systems

For supporting the technology enabling Smart Grid households, several requirements for the communication infrastructure is demanded. The WAMS requires the use of Mobile Cloud Computing for the SE operations, and it is strongly suggested that SE will migrate to a MEC service. To facilitate the communication between the RTUs, PMUs and the WAMS, URLLC is required for accurate and reliable observations for the WAMS to perform SE.

2.4 Financial Infrastructure

In everyday life, the critical function of banking and the financial infrastructure is overlooked by many. As seen in crisis times, the financial infrastructure is of paramount importance and criticality. For the population to obtain groceries, and business to survive, it is dependant on the financial infrastructure to function correctly. It is therefore essential to understand what this infrastructure requires to function. How will the requirements change with the implementation of 5G?

During the 2020 Corona-crisis, the importance of financial infrastructure was made abundantly clear to the general public. Seeing businesses heavy dependence on liquidity made it clear that a failure of even a couple of days in the financial infrastructure has devastating economic consequences, which has caused a cascading effect of bankruptcy and unemployment. Economics is an essential tool that allows governments to exercise authority and control crises, as well as ordinary situations. The functioning of this tool strictly depends on the functioning of the financial infrastructure.

However, there is little research on interdependencies in financial infrastructures. The lack of research is stated in the in-depth literature review from Ouyang [46]:

> «The applications of some approaches in the literature, such as agent based approaches, network based approaches, usually modelled two or only a proportion of the critical infrastructure systems and mainly focused on the critical infrastructure systems like electric power, water, gas and communication systems. Other critical infrastructure systems like banking and finance, commercial facilities, and government facilities, received relatively less attention. However, these critical infrastructure systems are of critical importance to disaster mitigation and recovery as well, and their integration can capture more types and more detailed descriptions of the critical infrastructure systems interdependencies in a comprehensive modelling framework... »

In the last century, financial infrastructure has experienced several technological revolutions. The financial industry was among the first to create communication networks (before the development of the internet), and implement the use of computers as part of their infrastructure. In regards to the approach to new technology, the banking industry has been on the bleeding edge, and there is reason to believe that the 5G shift is no exception [53].

It is challenging to predict how the 5G shift will affect financial functions. However, there is good reason to believe that the end-user of the financial services will take advantage long before a change in the core architecture. For understanding why it is a confident prediction, and understanding of the inner workings of the financial infrastructure is required. How a monetary transaction is technically executed in the financial infrastructure was explored in the pre-project of this thesis [21]. The transactions constitute the core dynamic of the infrastructure explained in Subsection 2.4.2.

2.4.1 Operational Failure in Financial Infrastructure

The literature on risks in payment systems has traditionally focused on credit and liquidity risk [46]. As most modern central banks have put in place measures to limit such risks (e.g. by the introduction of a central ledger system to limit credit risk, or throughput rules to limit liquidity risk), the focus has also moved to operational risk. Operational risk is the risk of loss resulting from failed internal systems, human error or external events such as deliberate attacks or natural disasters. As large-value payment systems allow financial institutions to settle obligations stemming

from financial market transactions, any disruption to standard payment settlement processing could constitute a threat to financial stability.

It is challenging to find models and operational data from financial infrastructure due to the traditional lack of focus on operational failure in this sector. However, scholars have, in recent years, been focusing more on the increasing cyber threat to financial systems [5]. The Basel Committee on Banking Supervision has since the early 2000s shed essential light on the lack of research on operational risk in the financial infrastructure [30, 41].

2.4.2 Core Dynamic

For the financial infrastructure to provide the critical function of transactions, there are three main categories of institutions that are critical. Figure 2.4 illustrates a case of transactions between two parties, which explains the different institutional relations of the financial infrastructure. The primary responsibility for the central bank is to control the asset amount in the financial system since this directly influences the currency value. Currency is no longer physically in the way it used to. The banking industry has developed sophisticated systems and networks to ensure that no new assets are introduced into the financial system. One of the measures is that all banks store their assets in the central bank through central banks accounts. In parallel, the banks have core banking systems to keep track of all accounts and assets stored in their bank. This mechanism makes transactions inside one commercial bank very quick since it only needs to be processed inside the core banking system. Small transactions between customers are also handled inside the commercial core banking systems by acquiring accounts in each other's banks.

For larger transactions, that may threaten the liquidity balance of these external accounts; the financial infrastructure uses the Real Time Gross Settlement System (RTGS). As explored in the pre-project of this thesis, when the size of the transaction reaches a certain amount, the RTGS must be used for credit security reasons. All commercial banks are required to hold accounts in the central bank so that large transactions can be settled internally in the central bank [21].

The second category of institutions is the commercial banks, which is the provider of most financial services to private individuals and businesses, ranging from loans to transactions. Including the core banking systems, the commercial banks are also responsible for availability through their end-user systems like mobile banking apps and web-bank applications. It is the end-user service that will be most affected by the 5G revolution, and it is reasonable to believe that the end-user services will extensively rely on the MCC functions of the 5G.

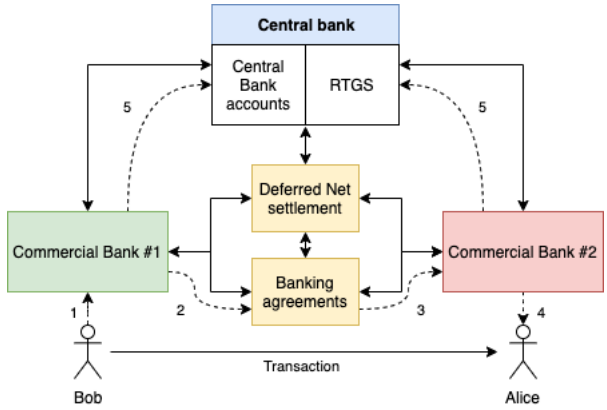

Figure 2.4: When making a transaction from Bob to Alice (customers in different banks), money does not flow between banks. Instead, messages are sent between the commercial banks (2,3), where the banks hold accounts with each other, and the transaction is processed internally. In large transactions, the RTSG is used to communicate between the commercial and central bank. Each commercial bank has accounts within the central bank, which are then balanced accordingly (5) [21].

The third category of institutions is the payment providers, which are essential in core banking infrastructure. They operate mostly on the user end; the interactions with the bank are becoming more and more digital. With the use of deferred net settlements (e.g. Visa, Mastercard, Paypal), other actors than commercial banks can facilitate payments between customers and service providers. This creates yet another web of interdependencies, inside and out of the financial infrastructure.

The 5G transition is predicted to increase mobile payments and mobile asset management [62]. One of the advantages with the 5G transition is its ability to facilitate data processing closer to the data source (customer), forcing a move from the central processing towards distributed processing of data [20]. Moving data processing form the central internal financial infrastructure to the 5G service would be a huge step, and make the financial infrastructure, even more, dependant on the communication infrastructure system.

2.4.3 Markets

From a technical standpoint, the market is a virtual service that facilitates the trade, in this case, of electricity. Today's economy is primarily related and dependant on the market where stocks, goods, services, and energy is traded at high frequency. The fluctuations in the energy market impact a large part of power production and control. Having centralised production of energy provides the ability to regulate production and demand to maintain stable prices. The transition to Smart Grid and

decentralised power production allows households to assume more control over their electricity consumption.

The Smart Grid technology that enables households to produce, store and consuming power will create a new power market dynamic. There is reason to believe the power market also will become more distributed with the rise of Smart Grid technology [18]. Some also implicate the use of blockchain as a technology for facilitating this kind of local energy market [39]. This implicates a tighter integration between the financial infrastructure and future power systems, which is further explored in Section 2.4.5. The future power markets are dependant on the financial infrastructure, which is a complex infrastructure. With the introduction of 5G, it is believed that more payment and customer/user interactions will be processed with the use of 5G services. The faster and more reliable connection between the bank and its customers will enable more frequent trading and asset management.

2.4.4 Authentication Services

Authentication services serve an essential function in a digital society. Many service providers, especially government and financial, rely on creating secure communication, and authentication of their users. Several authentication services have been developed to ensure that only authorised users can access services. In Scandinavian countries, these are centralised government developed services. They are providing two-factor authentication with the use of mobile phones. This service creates a dependency between the financial infrastructure and the communication infrastructure.

2.4.5 Implications of Distributed Ledger Technology and Cryptocurrency

Many controversies are surrounding the digital currency and distributed ledger technology(DLT). It is essential to separate the two from each other since the concept of cryptocurrency has severe political and economic implications and motives, while DLT is a tool which has a broad spectre of application areas.

The main reason cryptocurrency is regarded as an improbable element in the background of this infrastructure model is the fundamental change cryptocurrency implies on the current financial infrastructure and the unlikeliness that this will occur. A fundamental point in cryptocurrency is the separation of currency and state by rendering the central ledger (in the form of the central bank) obsolete. This separation implicates that nation-states would lose control over their currency and in turn, one of the governments most essential tools to regulate the economy. For this reason, a cryptocurrency is believed to have little impact on the importance of the current financial infrastructure.

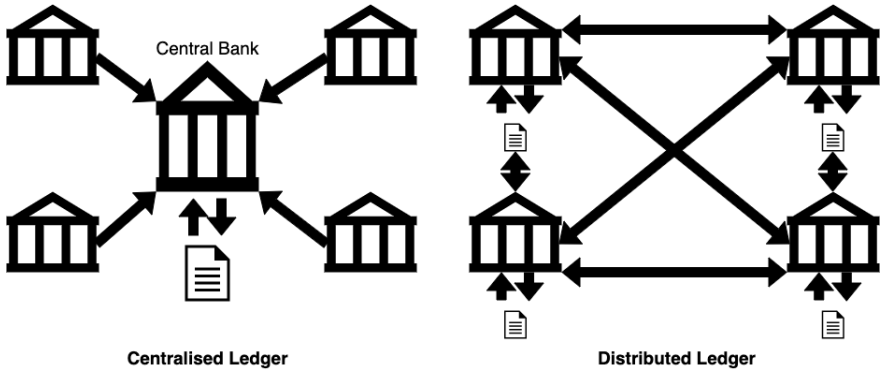

Figure 2.5: The main principle behind the distributed ledger technology eliminates the use of a central bank.

Distributed ledger technology, on the other hand, is a tool that has a higher probability of creating a shift in the financial infrastructure. DLT refers to protocols and supporting infrastructure that enables computing in multiple locations to process and validate transactions. The DLT can be used to keep the settlement system updated and synchronised across commercial banks, without central processing in the Central Bank, as illustrated in Figure 2.5. Put merely, DLT is a joint record shared by multiple computer systems across a network and can increase efficiency and security of the settlement process [10].

The financial technology (fintech) business is aiming at creating services connected the core banking systems, but deliver better or new user experiences on top of the commercial banks (this is enabled by the EU PSD2 act [17]). Some commercial and scientific papers suggest that a transformation to a DLT controlled by the central bank would save banks several million dollars each year in processing costs. In a Colloquium of the Belgian Financial Forum, it is stated that DLT could become an effective new way for a national currency to operate technically. They imply that it is possible to replace the RTGS system with a DLT system and preserve the central bank's control of the currency while still introducing the technical benefits of DLT [54, 31]. Using DLT in regulating a centralised currency may possible, and there are several reasons for doing so. The DLT could increase cost efficiency in payment processing, and create a more robust and secure financial system.

In Singapore, the government is looking into how the use of DLT could be a useful tool against money laundering and terrorism financing [34], which increases the probability of the implementation of such a system.

Even though there has been much buzz, and research has shown several upsides of implementing DLT in the financial infrastructure, no nation has implemented this so far. Several nations have publicly stated that DLT presents an exciting new opportunity for the financial sector, but it is implicated that this has to be driven by the private sector. Such a transition presents a huge investment cost and has a high risk of not providing the expected efficiency, making it unlikely that it will be implemented in the near future.

2.5 Research Question and Objectives

After studying the predicted developments of the three infrastructures, there is a great reason to believe that they are increasingly interconnected. Included in this increasingly interconnected future, is the development of invisible interdependencies that threaten the functioning of the infrastructures. In mitigating the risk of cascading failure in critical infrastructure, an essential question becomes:

What interdependencies may develop between the financial, communications and power infrastructures in the migration towards 5G and Smart Grid future?

This question is broad and challenging to answer. With a basis in this research question, several research objectives are developed to outline a method of research:

1. The initial step in achieving an understanding of the core functioning of the three infrastructures and how these are predicted to evolve
2. Choose a modelling approach based on a comparative analysis of different modelling approaches in this context
3. Designing and implementing a model that simulates cascading failures in these three infrastructures
4. Exploring interdependencies in and between the three infrastructures
5. Discussing advantages, opportunities and challenges with designing and modelling the three infrastructures using the chosen approach

Chapter 3
Method

There are numerous ways to describe and identify interdependencies in infrastructure. By describing the actions, dependencies and relations between the different entities in a system or infrastructure a model is developed. From modelling infrastructure systems and their interdependencies, simulations can be applied to study the different behaviours, and the effects of failure in components and subsystems have. These failures can lead to cascading failures in entire infrastructures that reveal unidentified interdependencies. In this chapter, the method for the modelling of the infrastructure systems is described. The chapters main focus is the choice of the modelling approach. Different modelling approaches are presented along with the argument for using an agent-based modelling approach for this model.

The choice of an agent-based modelling approach sets a frame for how the different infrastructure studies need to be analysed. Using the knowledge from Chapter 2, the agent-based approach provides a framework for the expected format in which the subsystems need to be described. This breakdown consists of simplifications, merging of different functionalities into components, or agents, and other estimations to include the necessary behaviour, but still maintains a certain level of abstraction.

3.1 Method Outline

The steps in the method of the thesis are summarised in Figure 3.1.

Figure 3.1: Outline of method steps.

The objective of this thesis work is to identify infrastructure interdependencies with the use of modelling. In setting the scope of this modelling, the first step is to create an initial case with a basis in a scenario which involves relevant emerging

technologies. The initial case of Smart Grid household transaction introduced in Chapter 1 establishes motivation and conditions for exploring the interdependence in three critical infrastructures in a relevant future scenario.

With a basis in the initial case, Chapter 2 presents state of the art research on the modelling and functioning of each relevant infrastructure. These studies form the foundation in this model. Studying literature on infrastructure and interdependency modelling also aids the selection of the modelling approach done in Section 3.2. After choosing the modelling approach and implementation tool, the model is designed. With a basis in the systematic development of agents, a study and estimation of expected behaviour in regards to agents failure rate are performed and presented in Chapter 4. Using these estimates to create values for the simulation is a crucial step for model accuracy.

The model implementation phase consists of developing the model based on the model design with the use of the JADE tool. After model implementation, the estimated values are initiated, and failure scenarios are simulated.

After running the simulation, the result is extracted, and by using a script, the model results are visually represented. The result is analysed, and different types of failures are identified in Chapter 5. Visualising the results gives an understanding of the consequences of failures in the different scenarios, which in turn can be discussed in light of the assumptions made in the model development. From analysing the failure events, and overall performance of the model, interdependencies are identified and discussed.

3.2 Modelling Options and Choice of Approach

The field of modelling interdependencies in infrastructure is still in an early stage, but there is an increasing focus on developing modelling methods to predict cascading failures accurately. The goal of this modelling is to discover interdependencies that may develop between three of the stated infrastructures. This requires the simulation of the future technical advances explored in Chapter 2, which can be considered subsystems of the infrastructures. In that regard, the research question and subsequent objectives provide expectations of a model with certain detail and abstraction level. Therefore a modelling approach that appropriately supports the modelling of subsystems in the 5G and Smart Grid architecture is required.

The most mature approaches for modelling interdependencies are considered: Input-Output Inoperability Model (IIM), Petri Net(PN), System Dynamics (SD), and Agent-based approach [46].

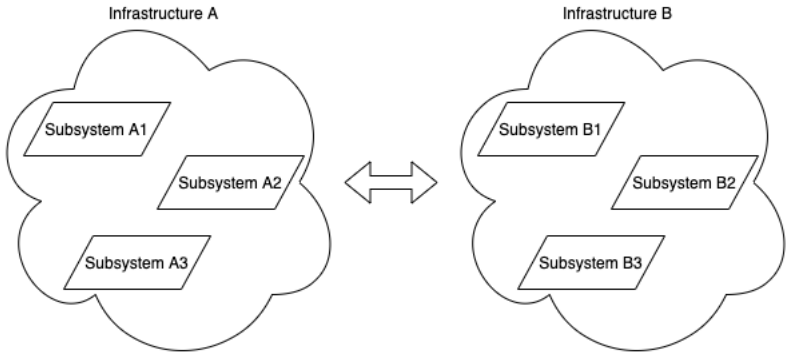

Figure 3.2: IIM is considered a holistic model, and considers infrastructures as monolithic structures, with limited interaction.

3.2.1 The Input-Output Inoperability Model (IIM)

The IIM is based on the Input-Output model extensively used in the field of economics. The Input-Output model was first proposed in 1973 by Nobel laureate Wassily Leontief for researching economic equilibrium behaviour between interconnected entities. In Input-Output based modelling the relationships of production between entities are described with the use of mathematical equations and models. This approach has since been applied to identify interdependencies between critical infrastructures. By defining the output as the risk of inoperability(failure) of the infrastructure, Haimes and Jiang developed the IIM [29]. Using the IIM to analyse interdependencies between critical infrastructures, it is possible to estimate the ripple effects of infrastructure failure on a general level [44].

As summarised in Ouyang, the IIMs are simple and effective in analysing how perturbations propagate among interconnected infrastructures and can help in the implementation and selection of mitigation strategies [46]. Since the IIMs are economic models, they are appropriately used in macroeconomic-level interdependency analysis. The IIMs is considered a holistic approach and as illustrated in Figure 3.2 it does not provide support for analysis of interdependencies at the subsystem level across infrastructures, which is of importance when analysing sub-infrastructures such as the 5G service and Smart Grids.

Even though this approach arguably provides high precision on a macroeconomic level, developing an appropriate mathematical representation of the infrastructures and their interconnection requires accurate and granulated data. These representations can be developed by analysing the aggregated behaviours of smaller interconnected entities.

3.2.2 Petri Nets (PN)

The PN approach is an approach explored in the pre-project for this thesis [21]. PN is a graph-based model made up of a number of places(P), transitions (T), input functions (I) and output functions (O) that represent the model with a four tuple: $PN = (P, T, I, O)$. This approach creates a network visualisation of the interdependencies between the infrastructures. Gursesli exemplifies the use of Petri Nets to model interdependencies in infrastructure in his 2003 paper [28]. Previous research states that this approach is restricted to the modelling of the psychical infrastructures and interdependence.

PN is assessed by Ouyang to have a high computational cost, as well as challenges with accessibility and quantity of input data [46]. In light of the challenges regarding the uncertainty of the final 5G and Smart Grid implementation, the required data quantity makes this approach arguably less suitable than SD, and agent-based.

3.2.3 System Dynamics (SD)

Similar to the IMM method, the SD approach also takes a top-down approach to the modelling challenge. Developed by Sandia and Argonne National laboratories, the SD approach is used to assist functional modelling and nonlinear optimisation techniques [65]. SD describes the infrastructure as a set of stocks(system states) and flows(describing the change in stocks) and indicating the connections and behaviour between them as feedback loops.

The pre-project to this thesis found that the SD approach captures essential causes and effects between infrastructures in disruptive scenarios and includes the policy and technique factors which impact the infrastructure systems in the long term [21]. It is mostly used for strategic investment recommendations and compare infrastructure protection strategies. Tweneboah applies this approach to assess security risk assessment of critical infrastructure [57]. This approach relies on detailed knowledge of the subject matter in creating the causal loop diagram, which is a semi-quantitative method. As with the agent-based approach, data is needed, and due to its sensitivity, it is hard to obtain. Ouyang estimates the accessibility of the required data for the SD is higher than the agent-based approach, but in turn, SD has lower computation cost [46].

The SD approach has previously been vital in enabling decision-makers to predict consequences from infrastructure failure. However, properly developing the SD model to acquire accurate consequence predictions requires calibration. This calibration demands vast amounts of data, something the Smart Grid and 5G subsystems have not yet produced, and data from the financial systems are hard to acquire due to security and privacy reasons. The SD approach is more appropriately suited for

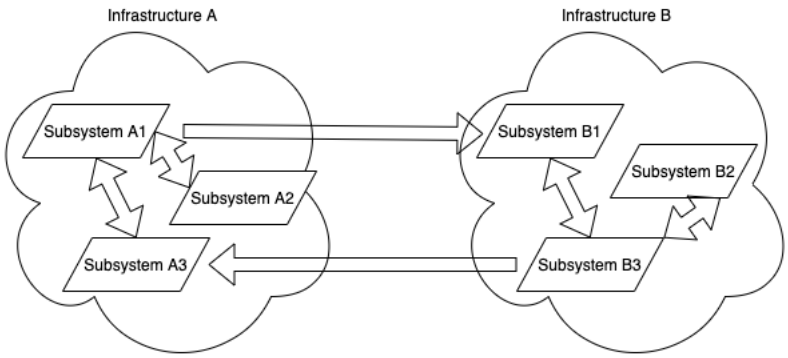

Figure 3.3: Unlike the holistic approach, the agent-based approach supports interconnections between subsystems within different infrastructures [44].

modelling the behaviour of infrastructures with the use of cause and effect reactions in catastrophic failure events. These weaknesses make it difficult to model the scenario described in the background using the SD modelling approach.

3.2.4 Agent-based

An agent-based approach is a bottom-up approach that assumes complex behaviour in infrastructure systems emerges from individual and relatively simple interactions of autonomous agents. Each agent interacts based on a set of defined rules, mimicking the real-world component, and simulates discrete events. The agent-based approach is dependent on the agent behaviour description, which is based on assumptions made by the modeller. Due to the support of breaking down infrastructures into its subsystems, it is not considered a holistic approach. Figure 3.3 illustrates how the subsystems within each infrastructure can be connected within and outside its infrastructure of origin. Considering how the 5G and Smart Grid infrastructure systems have multiple interconnections between different subsystem, the agent-based approach enables for the modelling of these smaller interconnections between subsystems. For example, how the Smart Grid is dependant on the 5G service for SE, and eNBs for providing connectivity for the smaller units in the Smart Grid.

Component assumptions can be challenging to statistically or theoretically justify. The calibration of the simulation parameters is difficult due to its dependence on real-life data, which is challenging to obtain from the actors in especially the financial infrastructure since it is of high sensitivity. However, the agent-based approach is flexible in this regard, and agent-based approach is widely used to model the infrastructure interdependencies, and used in similar modelling practise [45, 19]. Another advantage of the agent-based approach is that since it is considered one of

Approach	Pro	Con
IIM	Effective, precise and supports multiple infrastructures	Challenging development work, high data requirements and holistic structure
PN	High precision, and good support for visualisation	High computational cost, data requirements and limited support for cyber interdependencies
SD	High accuracy in results and support for event focused simulations	High abstraction level, data and calibration requirements
Agent	Flexible in regards to abstraction level, relatively low data requirement, high maturity	Mediocre computational cost, lower accuracy in quantitative results

Table 3.1: Summary of the modelling approach analysis

the most mature approaches within this field, there are several tools developed to support this approach.

3.2.5 Approach Summary

Table 3.1 captures a summary of the modelling approach assessment. When reviewing the selected modelling approaches, the agent-based is considered the most appropriate for this modelling. It supports a flexible model abstraction level, as well as enabling interconnected between subsystems. Also, the agent-based approach does not require extensive statistical data to provide results. The maturity of the approach and the assortment of tools supporting the approach may also provide a solid foundation for the model implementation process.

3.3 Choice of Implementation Tool

There are a vast number of software tools that are developed to assist in simulation and modelling agents and their behaviours, and this makes the selection of the most appropriate tool an interesting challenge [1]. In selecting the most suitable and appropriate tool for this modelling, the first step is to narrow down the list of potential candidates. This is done by filtering based on a functional and a technical requirement list. For this model the requirements are as follows:

Technical Requirements:

- Able to run preferably on Mac-OS (but VM can be used)
- Coding language: Java, Python, or JavaScript
- Model development effort: Moderate (Preference)
- Implementation platform: desktop/laptop computer
- Availability: Freeware

Functional Requirements:

- Agent-based modelling
- Heterogeneity in agents
- Support three different infrastructures (Telecom, Power, Finance)
- Facilitate high number of connections
- Agent attributes: Social ability, Autonomy, Reactivity

3.3.1 Technical Requirements

The constraints and requirements on the technical side are mainly due to available equipment. The limited budget demands software with macOS and desktop/laptop computer support and is available for free. The projects time frame also constrains the model development effort to a tool that is moderate in user effort. Continuous development, updated documentation, and an active community is also a factor that can contribute to lower the model development effort.

3.3.2 Functional Requirements

The functional requirements are based on the domain and approach of the modelling. Since the three infrastructures that are modelled are very different in state and behaviour, the tool must support the development of heterogeneous agents.

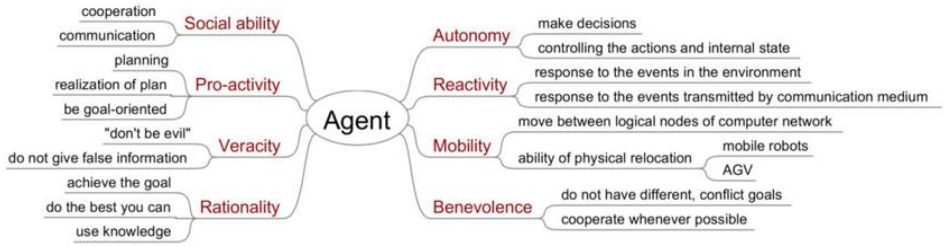

Figure 3.4: Illustration of the different attributes of agents in agent-based modelling [26].

By using Foits review of general agent attributes illustrated in 3.4, the required agent attributes for this model is defined [26]. It is defined that the software tool must

Software	Description	Evaluation
Eve [7]	A general multipurpose tool for modelling and simulation focused on scale-ability and online connectivity to create open world environments.	Does not have rich and available documentation and appears to have a more online focus than necessary for this project.
JADE [55]	Tool for developing distributed applications composed of autonomous entities.	Professional freeware from Telecom Italia. The last update made three years ago but has rich documentation and several user guides. JADE's documentation has over 3000 citations, which illustrates a high degree of maturity.
MaDKit [37]	Multiagent-based development platform written in Java that allows building distributed applications and simulations using the multi-agent paradigm easily.	Proper documentation and limited activity in the user forum, but is continuously updated (last update this year(Feb 2020)), and the developers seem easy to contact. The use of MaDKit facilitates high heterogeneity in the agent architectures, which gives freedom but may also create more development work.
Jason [32]	Jason is an interpreter for an extended version of AgentSpeak. It implements the operational semantics of that language, and provides a platform for the development of multi-agent systems, with many user-customisable features.	Last updated one year ago, the software is still in development. The Jason community is reasonably broad, with decent documentation.

Table 3.2: Final evaluation of the modelling tools that satisfy the technical and functional requirements.

support agents social ability, seeing as the dependencies represented as connections between the agents are the main focus of this simulation. Agent autonomy is important for simulating the reliability of the different model agents. The autonomy of the infrastructures subsystems is required to simulate different agent states, for example, a component failure, subsequently the agents must inhibit a reactivity attribute for the simulation of dependency and cascading failure. It is an advantage that the tool supports a holonic approach as infrastructures might depend on components within the system as well as the infrastructure as a whole.

3.3.3 Tool Selection

Using the defined requirements to review the literature and online resources the appropriate tools are narrowed down to four options that satisfy the technical and functional requirements [1, 63]. Table 3.2 describes the final evaluation of documentation, communities and other softer elements is used to make a final decision.

The JAVA Agent DEvelopment Framework (JADE) tool provides all technical and functional requirements. JADE is superior in regards to the available documentation and support for the tool. Even though it can be considered outdated with the last update is a year old, the forum activity and low response time from the community give reason to believe that this tool is not abandoned. In comparison with the other candidate tools, the JADE tool is deemed the most appropriate tool for this model implementation.

3.4 Modelling

After selecting the modelling approach and tool, the next step is the model design and implementation.

3.4.1 Model Design Method

From the background research summarised in Chapter 2 a UML-diagram describing the components and their connections is developed. This is done in several steps:

1. Taking basis in a simple UML case-diagram for each of the three infrastructures, describing their role in a Smart Grid transaction case.
2. Systematical review of infrastructure research (as summarised in Chapter 2), and developing a scheme over which subsystems each infrastructure model needs to include to provide the required functionality outlined in step 1.
3. Using research on interdependence modelling to decide which approach is appropriate for this model. This decision is discussed in Section 3.2.
4. Choosing the agent-based approach, the infrastructure subsystem scheme is reviewed to provide an appropriate abstraction level to the model. In this step, the agents that represent the infrastructure subsystem(s) are developed.
5. Using this scheme, the agents are connected in a UML-class diagram.

The material produced as part of steps 1 and 2 is used as stepping stones in the development.

Step 4 involves simplifying this scheme and is a challenging but necessary step since it is vital to find the appropriate granularity/level of detail in such a model partly to narrow the workload, but also to preserve the accuracy and still manage to produce relevant results. The simplification is in practise done by merging different subsystems, and their functionality into more compound subsystems based on their role concerning the initial case. By simplifying the different subsystems, limitations for the model scope is also set. These limitations are essential for obtaining more accurate results. By implementing too many components with too much functionality, more results could be obtained, but would naturally be less precise and require more time to analyse.

The UML class-diagram developed in step 5 is used as a basis for the model implementation. This diagram is quality assured by cross-referencing with the initial systematic research sheet which developed the different subsystems. The diagram also provides essential visual aid in the testing and analysis of the model.

3.4.2 Implementation Method and Principles

The implementation phase of the modelling consists of developing a simulator by the model design. The simulator is essentially a program that initiates the agent in a Java environment, provided by the JADE-tool (described in 3.3.3). The agent's behaviours and communication need to be programmed. Finally, the program needs to be initiated with the interconnections and the values according to the model design.

Using the JADE agent platform, the development is centred around creating an appropriate agent framework for the infrastructure model. One agent represents a system, or infrastructure entity, like a core banking system or a remote terminal unit(RTU). There are, of course, some differences in the agents, but the main functionality and logic are the same for all the agents which represent different entities in the intricate infrastructure systems.

In the model implementation, a variety of different frameworks and guides have been researched. Porcesllinies and Setolas papers have contributed with the following insight in creating an infrastructure model using agent-based modelling [48]. The infrastructure should be modelled starting from the macro-components which have specific and easily recognisable roles. The level of abstraction inside each agent should be sufficiently high so that the model can operate of incomplete or generic data (easing required accuracy in the data acquisition). Externally each agent should be as uniform as possible to ease the development of connections and networks.

Panzieri [47] suggests that fuzzy numbers should be used to code parameters and values. In this way, not only is it possible to represent vague statements such as

'component B depends very much on component A', but the results of simulations can also be analysed in terms of their vulnerability and exposure. These principles are applied in developing the main agent functionality to consists of a common uniform communication between the agents and a user initialised internal behaviour. By taking advantage of Porcellinis implementation of *operational level* (OL), a more detailed simulation can be achieved.

The agents' OL symbolises the infrastructure entity's ability to provide the expected service. Ranging from 0 to 1, where 1 represents the expected service of the infrastructure system and 0 is a failure to provide the expected service. The OL is influenced by internal failure, which is a consequence of the designed failure rate of the agent and the cascading failure in dependant agents. When the agent fails, the OL is set to zero. If the failure is internally caused, the agent must initiate a restoration before resuming a full OL. Subsequently, the failure (new OL equal to zero) is communicated to the other agent's dependant to the failing agent. The dependant agent or agents may fail as a consequence, thus creating a direct cascading failure. Another alternative is that the agent is dependant on many agents the dependant agents OL is reduced equalling the number of failed dependant agents divided by all dependant agents.

The agents are also equipped with a *Requirement value*(R), which symbolises the minimum level of expected service that needs to be provided for an agent to function properly. The relationship between the R and OL is that the OL has to be higher the initiated required OL for the agent to provide any service. Once the OL is below R, the agent OL is set to zero but will however not trigger a restoration, since this failure is a consequence of failure in a dependant agent. In this case, the agent is only restored after the required service of connected agents is restored. The R is used to introduce some robustness to the infrastructure system agents, as their fragility would in several cases be overrated by an immediate failure due to a connected agent. This can be exemplified by the WAMS ability to preform SE without all RTUs and PMUs at 100% OL. By setting an R of 0.7 for the WAMS, it will tolerate a drop in several RTUs and PMUs before failure.

As illustrated in Figure 3.5, the state of the agent is dictated by the OL. The OL is determined based on the incoming (OL.in) OLs of the dependant agents, as well as a failure rate which may cause agent failure.

3.4.3 Extracting Simulation Data

The JADE-tool does not provide any direct analysis tools. However, it includes some simulation recording functions such as a communication sniffer and a logger function. For observing this model which includes over 60 agents, the JADE-tool functions are not adequate.

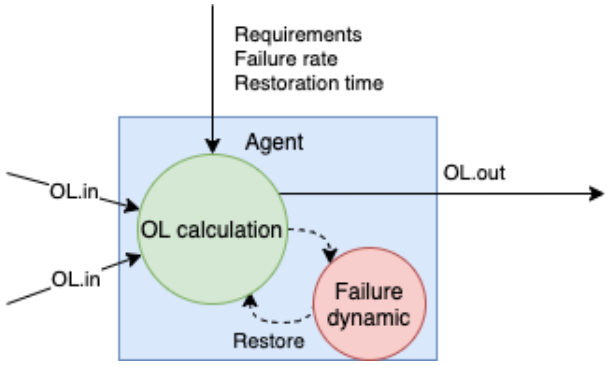

Figure 3.5: Scheme of the simple common agent design. The state calculation is based on two parts: comparing the OL of the dependant agents (normalised sum of the OL.in) with the required OL and the random failure probability of the agent. If the agent fails due to internal failure the agent failure-dynamic will pause the agent until it is restored.

The lack of direct analysis tools in JADE demands data to be extracted from the simulator in order to analyse the simulation result. Firstly there is a decision on what data to extract, and secondly, how will it be extracted. In this simulator, the data extracted is mainly the different agents Operational Level. The OL will show a failure of varying degree can propagate trough the infrastructure model.

The OL is logged along with agent details and timestamp. To save storage space and increase efficiency, this is only logged when a change in the OL occurs. This result is extracted in an XML format, and by developing a simple Python script, the data can be visualised in a graph. Analysing this graph can identify connections and interdependencies in the complex network of infrastructure subsystems by visualising cascading operational failures.

3.5 Simulation of Failure Scenarios

What interdependencies may develop between the financial, communications and power infrastructures in the migration towards 5G and Smart Grid future?

To answer this question, the initial case of a Smart Grid household that produces and consumes electricity based on a market dynamic is used to create several failure scenarios that are interesting to test with the simulation. In literature, most modelling scenarios revolve around a catastrophic failure, often due to extreme events like natural disasters and terrorist attacks. These scenarios are highly relevant but must be accompanied by an extensive investigation of internal fault factors such as system errors, component failure, routine failure and human operating errors

which occur at a much higher frequency and therefore pose a substantial risk in creating cascading failures. Malicious attacks are also of high significance and will be a factor in analysing the interdependence between the infrastructures. The case of operation failure concurrent with independent catastrophic events is also relevant for the identification of interdependencies, and are more appropriately simulated with the use of scenarios.

Developing a model can help study and analyse the severity of possible failure effects. For analysing the interdependencies, the initial case is used as a model context. With a basis in this context, different failure scenarios for each infrastructure is proposed and simulated to identify effects in a crisis scenario. The use of scenarios is inspired by Casalicchios work in analysing the interdependencies in the communication and transport infrastructure in the context of a burst in wounded citizens with different failure scenarios where faults and the traffic congestion was added to the infrastructures [14].

3.6 Validation

Validating models and simulations of infrastructure systems is a challenge. Compared to natural science, where hypothesis can be tested with experiments in a controlled environment, the field of infrastructure interdependency modelling is more uncertain. Due to the scope and critically of the systems modelled, it is incredibly resource-demanding to test infrastructure interdependency models in a real-world setting. Even though it is possible to evaluate individual dependencies by separate experiments without risking a failure of the entire infrastructure, the number of dependencies implicitly covered in this model is extensive. Therefore, it is assumed that the validity of the simulation result is assured as a consequence of a correct model with accurate assumptions and precise implementation. Unfortunately, this may create several failure sources in the results. However, provided the correct groundwork, well-reasoned assumptions, and overall precision in the components' behaviours, the model results provide valuable knowledge.

Chapter 4
Model Design and Implementation

This chapter presents the model design and implementation developed using the method and agent-based approach described in Chapter 3, and the insights gained from the infrastructure study in Chapter 2.

4.1 Components and Agent Design

Any model consists of simplifications. What simplifications are made is dependant on the amount of functionality proposed to be covered by the model. There are few studies aimed at modelling three infrastructures, while still trying to preserve the level of functionality required to give system architects insight into what scenarios should be mitigated. In that sense, this model may be considered as having a wide scope. This scope forces complex systems like the financial infrastructure and 5G architecture to be stripped down to a minimum of functionality, but still managing to capture the relevant behaviours occurring in the systems. An advantage of the agent-based modelling approach is that the level of abstraction and granularity can vary from infrastructure to infrastructure. It must also be noted that model development is limited by time and resource, which provides an overall constraint to the granularity of the model components.

The financial infrastructure is modelled with little granularity and high level of abstraction. This is due to several factors: (1) the limited research done on operational risk creates a challenge in finding appropriate data on modelling architecture and reliability data. (2) There is a variation in the architecture of financial infrastructure, which makes it most appropriate to maintain a high abstraction layer to make the model applicable to several financial infrastructures. (3) The financial infrastructure is vast, and only a small part provides the functionality required by the initial case. However, the system is tightly interconnected, and by taking such a limited section of the infrastructure, several factors that may be important to some subsystems may not be accurately represented. By applying such low granularity, the simulation will

be limited in concluding the vulnerability and exposure of subsystems with high precision. This will, in turn, limit the potential for accurate mitigation measures.

The communication infrastructure is modelled with slightly more granularity than the financial, especially concerning the 5G. The 5G network and components are challenging to model, as reviewed in Chapter 2. However, it is the infrastructure that ties all others together, making it essential to include with higher granularity. The model granularity of the electrical power infrastructure is twofold, similar to the communication infrastructure. The Smart Grid implementation is provided with more granularity since it is the focus of this model.

In relation to other models of infrastructures interdependencies and dependencies between one or two infrastructures, the abstraction level is quite low. However compared to models identifying interdependencies between several infrastructures using different approaches, this model provides high granularity. Identifying more than 4-5 components per infrastructure in a model with a similar scope size is not usual in previous works.

The advantage of such granularity, compared to the other approaches, is that conclusions and mitigation strategies can receive more precise data. This granularity does, however, demand higher quality in data. There is also a greater need for estimations and assumptions in a model with such granularity. This need impacts the accuracy, relevance, and applicability of the results.

How the agents are defined lays the foundation for what is perceived as the model's abstraction layer. There are countless numbers of possible abstraction layers when modelling such complex systems. In this case, when referring to components of a subsystem with a set of functions and responsibilities, these components are represented as an agent, or an agent may represent several components. This chapter describes the assumptions, estimations and decision in regards to the agent development. Essential aspects of the agent behaviours that need to be addressed for this model are the expected failure rates, which has a significant consequence for the model result. This chapter presents the process of agent development and the justification of the behaviour.

The *failure rates* of the agents are important for the steady-state simulation of the model. The failure rate is as mentioned in Section 2.1.2, the frequency at which a component is expected to fail. For this simulator, the failure rate is measured by failures per days of operation($days^{-1}$). It is, however, challenging to find accurate data sources on the failure rate of all components. To solve this challenge, the model uses three failure rate levels to describe some of the components failure rates. Table 4.1 presents the three failure rate levels. The levels are set based on estimates used in other literature and is assessed relative to each other.

Failure rate	**Value** ($days^{-1}$)
Low	$1 \cdot 10^{-5}$
Medium	$1 \cdot 10^{-4}$
High	$1 \cdot 10^{-3}$

Table 4.1: List of common values of estimation for component failure rates.

The *restoration time* represents the amount of time the agent uses to restore full OL in the event of internal failure. As discussed in Section 8.1 and 3.5, the restoration time variable may be used to simulate different failure types. In the steady-state, the restoration time represents a repair time of half a day and is set constant for all agents.

4.1.1 Model Design Overview

All components and their connections are presented the UML diagram Figure 4.1. The agents are grouped in boxes which are referenced in the following subsections for easy readability. This diagram is used as a design map in the implementation of the model. It also provides the reader with a better understanding of the model described in the next sections.

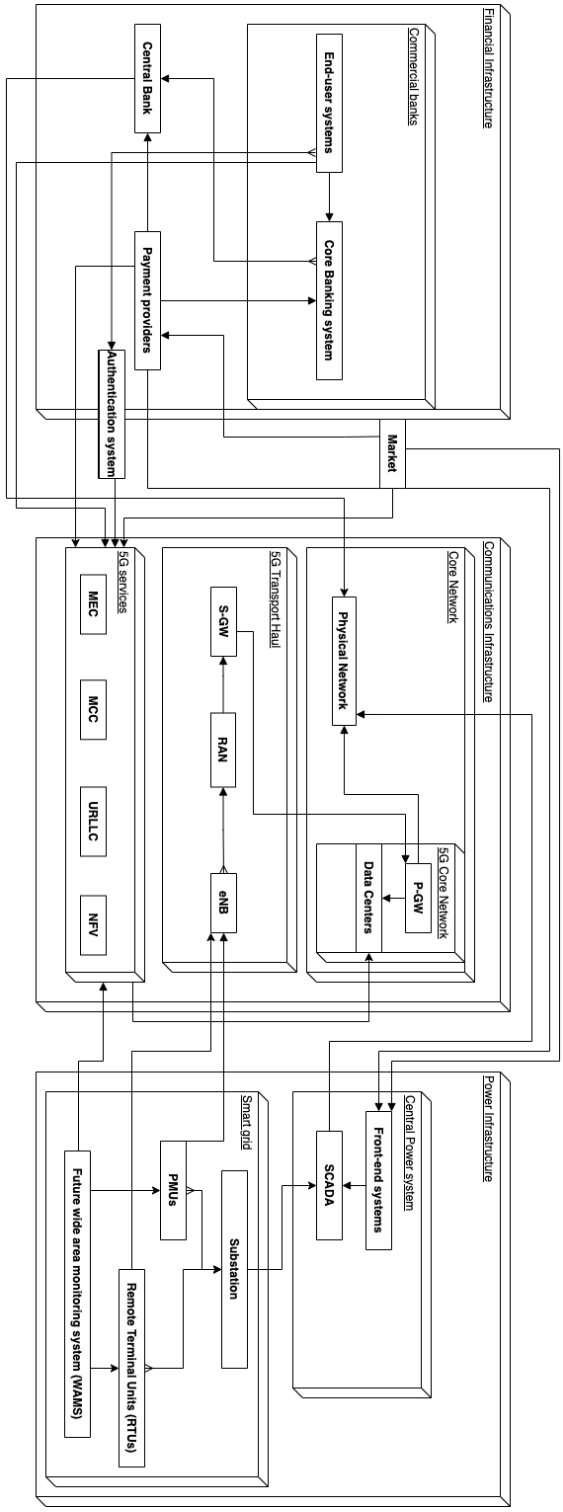

Figure 4.1: UML diagram of the model.

4.1.2 Communication Infrastructure

The communication infrastructure is modelled in three blocks, the core network, the transport network of the 5G, and the 5G services. These are considered the three main blocks in the 5G architecture as studied in Chapter 2.

Core Network

The core network is modelled two-fold, the communications infrastructure core network, which is comprised of the physical network and the 5Gs core network. The *physical network* agent represents the physical cables, routers and switches that make up the internet. Since the physical network is a very redundant system, being a distributed network is has few bottlenecks and central control. The failure rate of the physical network is, therefore estimated as very low. The physical network, which in some cases represents the internet, is a challenging functionality to introduce in such a model since it is reasonable to argue that all components are in some way dependant on the internet. Components dependency on electricity is in a similar position. The cases of failure in electricity infrastructure or the internet are unusual, but given the abstraction level of this model, these cases cloud the possibility of gaining more nuanced results form this model. However, this model separates the internet from the physical network, in that physical network is only critical for the operations of SCADA and central bank communications as well as the 5G operations.

Due to the sheer complexity and uncertainty regarding the 5GCN architecture, this model designs the *Packet Data Gateway (P-GW)* agent to represent more than just the gateway between the 5G mobile network and the numerous internet service providers. This agent also represents the 5G Core Access and Mobility Management Function (AMF). The remaining functionality of the 5G control systems are considered important for the 5G infrastructure, but less important for the initial case and is therefore gathered in one agent. (This functionality was provided by the Mobility Management Entity(MME) in the 4g/LTE architecture, along with other sub-functions mentioned in the appendix Table A.2 [22].)

Data Centres are the extensive facilities in which data is stored and processed. The data centres are the physical computers that provide virtual functions of the 5G service and functionality represented by the P-GW. The decision of including the data centres as a separate agent, and not as part of the P-GW, is precisely due to the physical nature of these systems.

The data centre agent is therefore critical to the 5G infrastructure and needs to provide high reliability. Reliability in data centres is defined in tiers by the Uptime Institute [58]. The 5G will certainly require data centres of at least Tier 3 availability, of 99.982%. This constitutes that the failure rate of the data centre is estimated

similar to the physical network, $6 \cdot 10^{-6} days^{-1}$. Similar failure rates have been assigned in other models of data centre availability [43].

5G Transport Network

The transport network of the 5G architecture is the section that provides mobile units connected to the internet. This section is comprised of three agents: the Service gateway (S-GW) which forwards data to the P-GW for further processing, the eNBs which are the wireless access points for the mobile units to connect to, and the radio access network(RAN) connecting several eNBs to the S-GW.

The *Serving gateway* (S-GW) agent provides the connection to the core network along with the *Radio Access Network* (RAN) agent which works as a connector for several eNBs. As explored in Section 2.2.1 there is consensus around the required performance for these components. These segments of the 5G network are expected to have extremely high reliability, and thus, a low failure rate [9].

The model is initialised with three *eNBs* based on the necessary amount of eNBs to provide coverage to a Smart Grid. The failure rate of the eNBs is estimated based on several data sources. One of which is the handover failure rate, which is by previous simulation results optimistically placed around 1% [35]. The failure rate is adjusted for the situations that multiple agents are connected to one eNB, which in reality would not require many handovers. Relative to the other component failure rates, this is to be considered high.

5G Service

The 5G service agent is a merge of all the 5G services into one agent. Several agents rely on the 5G service, making it a vital component in the model. It is dependant on the data centre agent since the physical location of the 5G service is inside the data centres. The 5G service agent represents the software services planned for the 5G to provide. Estimating the failure rate for this agent is done by using the reliability numbers presented in the NGMN 5G white paper [20]. It states that the 5G will provide ultra-high reliability of 99.999%, or higher for the use cases that demand it and therefore, the failure rate is estimated to be very low.

4.1.3 Financial Infrastructure

With the insight obtained in Chapter 2, the initial case provides some requirements for the financial infrastructure that is used for developing the different components in this infrastructure. Even with this narrowing, the abstraction level in the model of this infrastructure is still high as a consequence of the limited available technical insight into this infrastructure.

Commercial Banks

In the model, there are four initialised commercial banks. Based on the number of banks in western countries today, it is reasonable to assume that four banks would represent the number of dominating banking systems. This might seem incorrect to the reader, but most commercial banks are hosted in existing larger bank systems. A similar dynamic to the service providers in the communication industry, which runs their services on top of existing infrastructure. Each commercial banks consist of a complex number of subsystems. In this model, the commercial bank consists of two agents representing the end-user system and core banking system. They are separated since their behaviour and expected failure rates are vastly different.

The *end-user system* depends on customers being able to authenticate themselves (dependency on the Authentication system agent). As studied in Chapter 2, it is expected that the end-user systems will exploit the services of the 5G in the future, creating a dependency. The end-user system is naturally dependant on a functioning core banking system to provide the required functionality to the customers. An end-user system is continuously under development, and new functions are continuously explored and tested. This creates a high risk for common cause failures. As explored in Aldasoro 2020 paper on operational and cyber risks in the financial sector operational risks, a study with a comprehensive data set, the occurrences of operational failure are high. However, Aldasoro found that failures are often minor and not discovered and corrected for long periods of time [5]. To find more exact numbers, Abdymomunov technical report on U.S. Banking Sector Operational Losses and the Macroeconomic Environment reveals that operational losses due to events in the categories «Damage to Physical Assets», «Business Disruption and System Failures», and «Execution, Delivery, and Process Management»accounts for 36% of losses which acknowledges the high failure rate [2].

The *core banking system* is the heart of the bank, and it is a robust system with a long legacy. To provide its expected service, it is dependant on the central bank, as explained in Chapter 2. Using the results from the «experience with the Analysis of the Data Collected»by the Basel Committee, it is reasonable to estimate that the internal failure rate is considered low [41]. From the reports used in the estimation of the end-user systems failure rate, it is possible to assume that since very few of the banking failures are significant, the core banking system is providing high reliability.

Central Bank

The central bank is an essential agent for commercial banks and their core systems. For the central bank to provide the expected service, it is dependant on the physical network for the communication between its connected agents. Due to the critical nature of the central bank, it is considered to have a low failure rate. There is research

to be found on agent-based simulation of the RTGS-systems. Morten Bech explores operational failure scenarios in the chapter of «bank failures in large-value payment systems»and concludes that the operational fail scenario has a low likelihood but with significant consequence for the commercial banks' core systems [10].

Payment Providers

Payment providers are also an important middleman between the commercial banks and in this case, the power systems. This agent is, however, a generalisation, and simplification. The payment providers also work as a middleman between the commercial banks and the market when customers plan transactions. According to Heinrich paper from 2006, there are several recorded events of payment systems in the Nordic countries suffering catastrophic failures [30]. It is, therefore, reasonable to assume the payment providers have an average failure rate compared to the other agents in this infrastructure.

Market

A market is a platform that enables transactions of goods and services. In this model, the market agent represents the virtual electricity market. There is reason to believe that the market will evolve to be an integrated part of both the Smart Grid and the 5G service. Vital to the reasoning of including this component is its fundamental role in creating interdependencies between the power and financial infrastructure. There is good reason to assume that the production and consumption dynamic in the smart gird is heavily impacted by pricing set in the electricity market. The market agent is estimated to have a medium failure rate based on the nature of similar digital services.

It can be discussed that a crash in the market would create escalating and cascading failures in Smart Grid production. However, these are connections that are challenging to model appropriately, but some solutions are proposed in the discussion chapter.

Authentication System

The authentication system agent is meant to represent an emerging trend of public centralised authentication systems for the digital space. In Scandinavian countries, these are well established, and many critical services depend on them. Among others, the banking systems. It is also reasonable to speculate that power companies also will depend on this form of authentication of their customers, but that is not addressed in this model. It is reasonable to assume that the authentication systems will extensively integrate with the 5G services. Their observed failure rate is hard to estimate due to the lack of research on these kinds of systems which is natural, considering the

limited use of centralised authentication systems. In nations where these systems are implemented, experience shows a highly reliable service with a low failure rate.

4.1.4 Power System Infrastructure

The power systems are in this model made up of two main blocks of functions. The central power system, which in many ways represents the current architecture of power systems, is connected to a Smart Grid system. Since the Smart Grid system is in the focus of this modelling, this subsystem is provided with more detail than the central power system.

Central Power System

Controlling the power system is the primary *SCADA* system agent, which is the central controller in the power system infrastructure. The SCADA connects with its sensors via the physical network but serves several other agents trough cyber and logical dependencies. Due to its critically, the SCADA systems have been the topic of several infrastructure models [13, 36, 40]. Even with high focus from external adversary actors, the SCADA system is estimated to provide reliable services, with a low failure rate.

Front-end Systems is an agent representing the electricity systems behaviour via an interface towards the customer (power production data), payment provider(billing) and the market (production and consumption data). Similar to the commercial banks' mobile applications, the electricity company has auxiliary systems that are more flexible and would naturally suffer from a higher failure rate. The front-end system is dependant on the data provided by the SCADA. The market and payment providers are logical and cyber dependant on the information provided by the front-end systems of the power infrastructure.

Smart Grid

The model includes one initialised Smart Grid. State Estimation in the Smart Grid requires a setup of a WAMS connected to PMUs and RTUs, which again is connected to the central power through a substation. The substation is an agent depending on the SCADA system of the central power system.

It is assumed the Smart Grid in its initial phases will contain both PMUs and the legacy measurement systems of RTUs. To model one Smart Grid, a set of 30 RTUs and 10 PMUs is initialised. These units will both depend on eNB connection to convey their measurement data to the WAMS. Since the RTUs are considered an older system, it is assumed that their failure rate is slightly higher than the PMUs. According to Wangs PMU reliability model and evaluation method, the

PMUs availability is estimated to be 0.99833 [60]. From this, it would be reasonable to estimate a medium failure rate.

Exploiting PMU inputs by robust, decentralised and real-time SE solution calls for a novel communication infrastructure that would support future Wide Area Monitoring System (WAMS). The WAMS is logically and cyber-interdependent on the PMUs and RTUs in the Smart Grid, to counteract disturbance on the grid. For performing complex processing state estimation, the WAMS is dependant on edge cloud computing provided by the 5G service [18]. Scholars have estimated the availability of the WAMS to be 0.998842, an estimation that included an induced failure by the PMUs and RTUs. Therefore it is reasonable to assume the internal unit itself has a higher availability [61, 66], and the WAMS agents failure rate is therefore estimated as low.

4.1.5 Model Design Summery

Table 4.2 summarises the component designs, and is the foundation of the UML diagram in Figure 4.1. A more in depth table with additional components left out of the final model, see Appendix A.3.2.

4.2 Simulator Overview and Implementation Notes

The simulator is developed in the Java Agent Development Environment(JADE), using the Eclipse IDE [55, 27]. The components identified and designed in Section 4.1 are initialised as agents in this simulator. The process of initialising the components appropriately in JADE-environment is described in the proceeding sections along with snippets of core agent code. Appendix A.3.2 contains more elaborate source code. Figure 4.2 illustrates the relations between the different environments, platforms and components essential for the simulator.

4.2.1 Agent Implementation

Following the implementation principles described in Section 3.4.2 a common *entity agent* class was developed. This class inherits functionality from the JADE tools *Agent* class, which enables initialisation to the JADE agent management system (AMS) environment along with the ability to add agent behaviours and communications between agents.

With this custom entity agent class, a more specialised framework for all the agents in the simulation is provided. The class is characterised by giving the agent's failure(and restoration) mechanisms, communication setup and operational level calculations. Following the implementation and design, each agent must be initialised with a failure rate, restoration time, and the agent which depend on this agent.

Component	**Dependencies**	**Failure Rate**
Market	Front end service(power), Banking, payment providers	Medium
Central Bank (RTGS)	Physical Network	Low
Authentication	5G Service	Medium
Core banking system	RTGS	Low
End user systems	5G Service, Core banking systems, Authentication systems	High
Payment processors	Central Bank, Core Banking systems, Front end service (power)	Medium
Physical network		Low
Data centers (DC)		Low
Packet Data Network Gateway (P-GW)	Physical Network, DC	Low
Radio Access Network (RAN)	S-GW	Low
eNB	RAN	Medium
Serving Gateway (S-GW)	P-GW	Medium
5G Service	DC	Low
Front end service	SCADA,5G Service	High
SCADA	Physical Network	Low
Substation	SCADA	Low
Phasor measurement units (PMUs)	WAMS, eNB	Medium
Future wide area monitoring system (WAMS)	PMU, RTU, 5G Service	Low
Remote Terminal Units(RTU)	eNB, Substation	Medium

Table 4.2: Overview of the initiated agents with dependencies and failure rates.

The inherited JADE agent functionality enables the agent behaviours to be added. The behaviours can be of three types depending on their execution: cyclic (repeating forever), sequential, or ticker. To understand how the agents for this model are implemented, three core methods are reviewed.

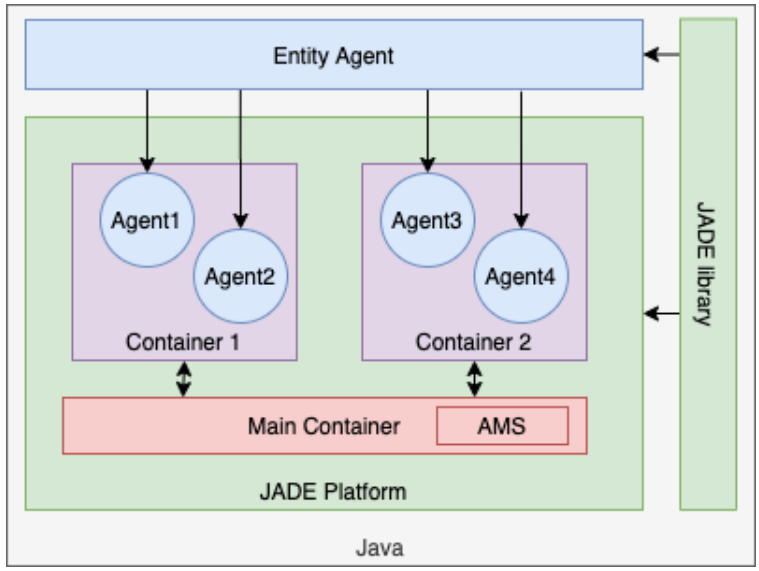

Figure 4.2: The JADE Platform provides a java environment for the agents, and the JADE library is utilised by the entity agent class and JADE platform. The entity agent class is developed for this model and provides a basis for the agents behaviour. The agents are organisationally grouped in containers that may be used for collective termination of the agents. Agent communication is enabled by the AMS which is initialised in the main container of the JADE platform.

OL Calculation

The first initiated behaviour is the *restore check*. For every 10 milliseconds, this method calculates and updates the current OL of the agent, based on the incoming OLs of the surrounding agents. Sequentially, the OL is compared with the required OL level (R), which may trigger an agent failure.

```
TickerBehaviour restoreCheck = new TickerBehaviour(this, 10) {
 public void onTick() {
    //Calculates the agents current OL by summerizing the recieved
    //agents OL and divding by number of connected agents
    double totalDependencies = getInConnectedAgents().size();
    totalOL = getInConnectedAgents().values().stream().
    mapToDouble(Double::doubleValue).sum();

    ...

    setOL( totalOL / totalDependencies);
```

```
    //checks if the OL is over the required level (R)
    if(getOL() < getR()){
        setOL(0.0);
        System.out.println(getAID().getLocalName() +
        ": Suffered a failure due to low Operation Level.");
    }
    //Internal failure triggers restoration procedure
    if(isF()){
        restoration();
...
```

Agent Communication

The agent communication is a vital aspect of the model implementation. Communications between agents are enabled by the JADE AMS and the protocol in line with the FIPA 2000 ACL(Agent Communication Language) Message Structure Specification standard [11]. The agents OL is sent to the agents that depend on it, every time it is changed. Upon receiving the OL of an agent, agent A calculates its internal OL by summing the incoming OLs and dividing it by the number of agents that agent A depends on giving the agent an OL equal to the average of all dependant agents.

The class method of sending the OL to the user-initiated agents' connections is presented below. This method is called each time the OL setter is called.

```
private void sendOL() {

    for (Entry<AID, Double> Agent : getOutConnectedAgents().entrySet()){
    ACLMessage msg = new ACLMessage(ACLMessage.INFORM);
    try {
        msg.setContentObject( getOL() );
    } catch (IOException e) {

        e.printStackTrace();
    }
    msg.addReceiver( Agent.getKey());
    send(msg);
   }
    ...
```

The agent's receiver method is a cyclic behaviour initiated in the agent. Upon receiving an INFORM message, the sender is stored as an *in connected* agent. The in connected agents is a hashmap of all connected agents and their most recent OL. By using this hashmap, the agent is able to calculate its own OL.

```
CyclicBehaviour reciever = new CyclicBehaviour(this) {
public void action() {
  ACLMessage msg = myAgent.receive();
  if(msg != null) {
    if(!getInConnectedAgents().containsKey(msg.getSender())) {
     getInConnectedAgents().put(msg.getSender(), 1.0);
      }

    if( ACLMessage.getPerformative(msg.getPerformative()) == "INFORM"){
      try {
      getInConnectedAgents().replace(
      msg.getSender(), (double) msg.getContentObject());
      } catch (UnreadableException e) {
        e.printStackTrace();
...
```

Failure and Restoration Dynamic

The final important aspect of agent behaviour is the internal failure and restoration dynamic. Pseudorandom failure with a set frequency is achieved by using the random next double function and comparing it with the initiated failure rate.

```
TickerBehaviour failureCheck = new TickerBehaviour(this, 10) {
@Override
protected void onTick() {
    // Checks if the agent fails or not
    if(new Random().nextDouble() <= getFailureRate()){
     setOL(0.0);
     setF(true);
    System.out.println(getAID().getLocalName() +
    ": Suffered an INTERNAL failure.");
...
```

The restoration method is called by the on tick behaviour restoration check. The dynamic merely is halting the agent for the restoration time period, upon which the OL is reset to one, and the failure boolean is false.

```
private void restoration() {
    try {
     Thread.sleep(getRestorationTime());
    } catch (InterruptedException e) {
     e.printStackTrace();
    }
    setOL(1.0);
    setF(false);
    System.out.println(getAID().getLocalName() + " Restored");
}
```

4.2.2 Model Initiation

The initiation of all agents is done according to the model design in a *infrastructure model* class. By utilising the entity agent class, the model is initialised with all connections and parameter values as presented in Section 4.1.

4.2.3 Time Management

The simulator logger logs the system time of the changing OL events, the time management of the simulator is dictated as the system time in milliseconds. The on tick behaviour of failure check is initiated to check every ten milliseconds which symbolises a day in real life.

4.2.4 Testing and Debugging

Although validation of the model is challenging, testing how the simulation is working compared to the expected behaviour of the model is essential. Looking at individual segments of components and the OL reaction reveals implementation errors or bugs in the simulation. As seen in Figure 4.3, it is expected that the failure of two eNBs, will propagate failure to the WAMS. Studying the second failure of the WAMS, we observe that the individual failures of eNB-0 and eNB-1 influence the OL of the WAMS with some delay. This failure is due to the propagation via the PMU's, which depend on the eNBs. By repeating this for several segments, it can be reasoned that the model's implementation is coherent with the model. By using this visualisation of the result, some uncertainty in the analysis can come from the challenge of not knowing what the cause of the reduced OL is. However, the possibility of a common cause failure occurring during, under or after experiencing a cascading or escalating failure is low and does illustrate a possible real-life scenario.

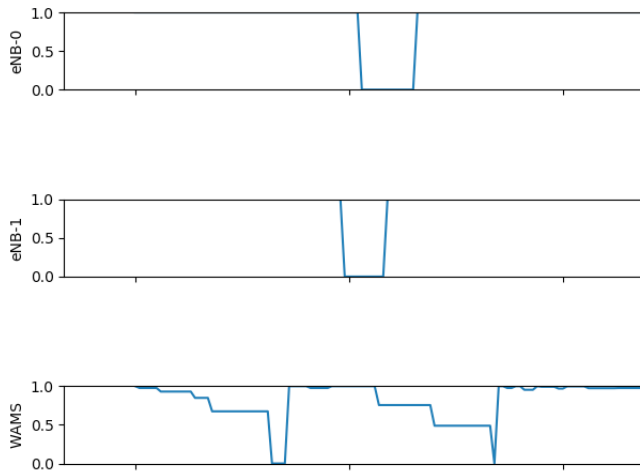

Figure 4.3: Analysing an expected cascading failure reaction occurring in the simulation. The WAMS experiences two failures, were the second failure can be assumed to be directly caused by the eNB failures.

Chapter 5
Results

In this chapter, the simulation results are presented and discussed. A simulation is run using the simulator with initial values detailed in Chapter 4 to obtain steady-state results from the infrastructure model. Afterwards, different failure scenarios are simulated and discussed individually.

5.1 Steady State Simulation Results

Simulating with the parameters described in the previous chapter creates statistics which is used to analyse the model performance. With a basis in the estimated scope of the component failure rates, which defines a low failure rate as a failure occurs once every 274 years, appropriate simulation time is set to approximately 7000 years. This simulation time-frame is considered adequate to produce results accurately representing the steady-state of the infrastructure systems behaviours. The Appendix A.1 includes the plots from a steady-state simulation of 700 and 2000 years which show consistent results.

The OL represents the agents ability to provide the required functionality. We observe the components exposure to cascading failures by analysing the mean OL from a simulation with a long time frame, as seen in Figure 5.1. The standard deviation(STD) of the OL values tells how frequent the agent was experiencing a state of failure(high STD) versus a slightly reduced OL(low STD). With the use of these analysis, the exposure and vulnerability of agents may be identified.

Figure 5.1 shows the mean OL of the agents in a steady-state simulation of approximately 7000 years. The market agents demonstrate a significantly lower mean OL, compared to the other agents. This reduced OL is not clear in Figure 5.1, but by calculating the standard deviation of the OL of each agent, we can more easily observe differences in the agent performance. The market agents standard deviation displayed in Figure 5.2, confirms the number of reduced operations it suffers.

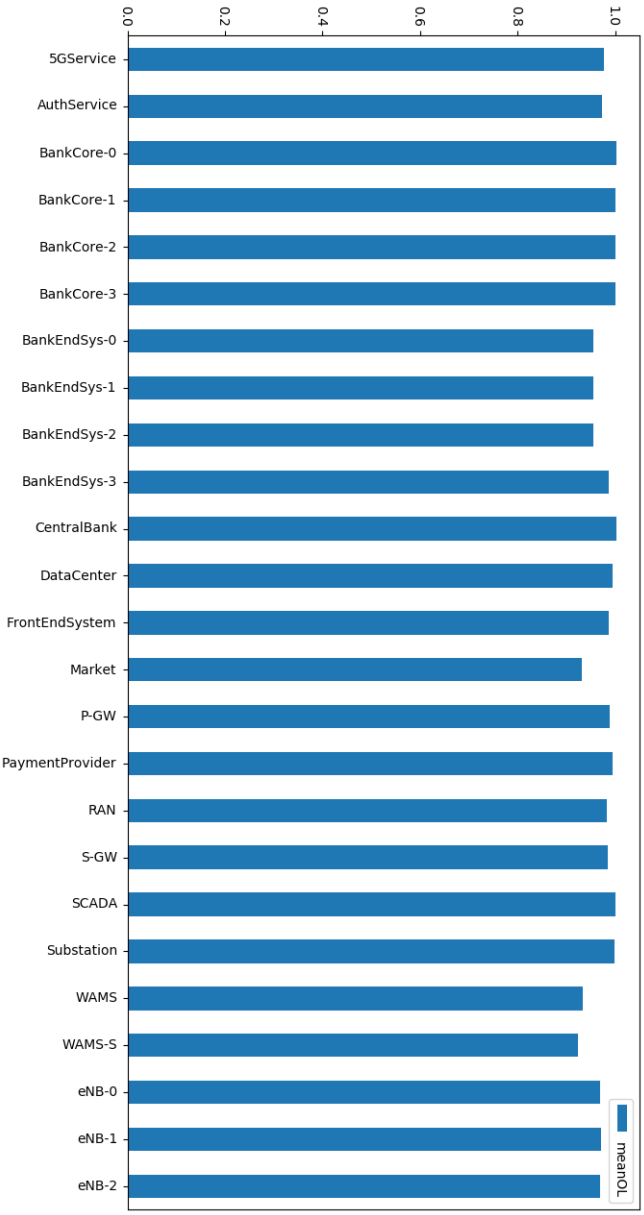

Figure 5.1: Mean OL in a steady state simulation of 7454 years.

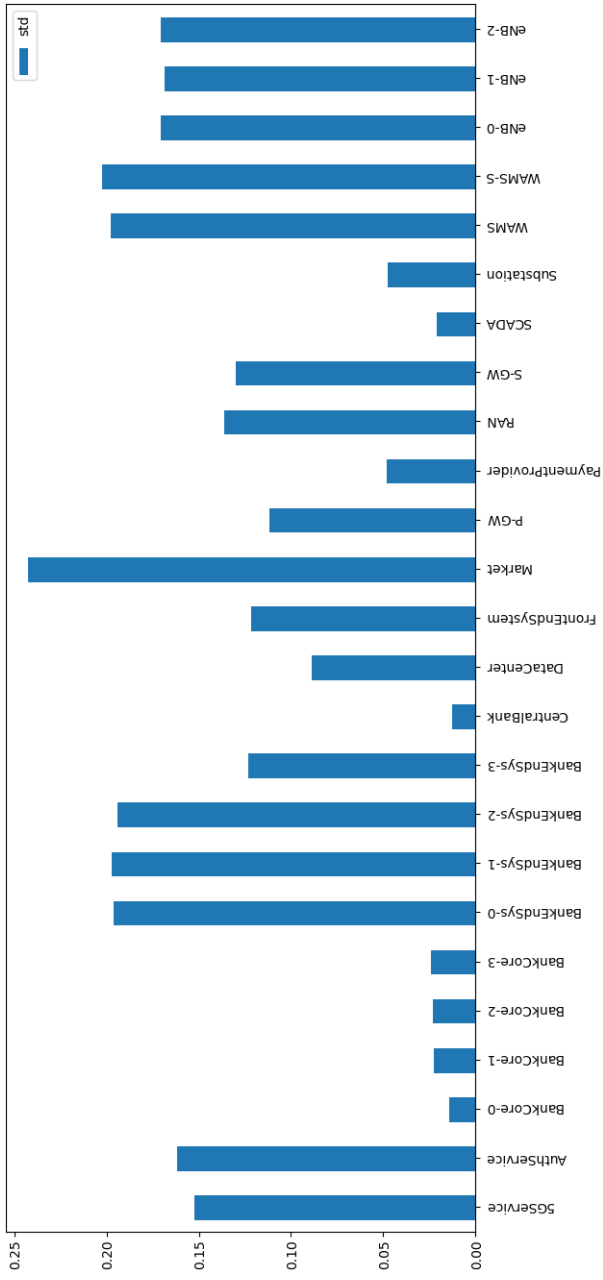

Figure 5.2: The agents standard deviation in OL values in a steady state simulation of 7454 years.

Since the market component is showing such an exposed position, an effort to decentralise the functionality of the market, as suggested by [39], might reduce the consequences and subsequently, the risk of cascading failure. As discussed in the central bank scenario below, it is reasonable to assume that the market component inhibits a substantial amount of economic and social-behaviour dependency, especially in regards to the production in the Smart Grid.

Connected to the market agent is the payment provider agent, which is observed with a mean OL of 0.949975. This is lower than expected for an agent with a medium failure rate, and it can be argued that this is due to its dependence on the three banking end systems.

The implications of the result for the initial case makes it reasonable to argue that households that play an active part in the Smart Grid are greatly affected by the interdependencies within the three case infrastructures. Especially the market which provides a trading platform is an essential factor for households. Analysing the results of the simulation provides arguments for a debate around the interdependencies created by the 5G and Smart Grid evolution.

5.2 Scenarios

It is challenging to obtain results from this kind of simulation in a format that enables easy analysis. Interdependencies are both challenging to display and analyse. The results from the simulations are extracted in the form of a trace of agents OL. As explained in Chapter 3, this data is processed by scripts and displayed as individual sub-plots for each component. Analysing all component traces poses a significant challenge due to the number of components in this simulation. This challenge is mitigated by displaying them in sub-plots and analyse them in groups with a basis in the scenarios. These scenarios highlight how catastrophic failures cascades trough the infrastructures and thus can be analysed as possible chain reactions to mitigate.

Catastrophic failure is simulated by increasing the restoration parameter in the relevant agents. The failure rate is also increased to provoke a failure event.

Scenario Context

The initial scenario provides the context of the simulations. The introduction of Smart Grid technology is predicted to provide households with the ability to become both producers and consumers of electricity. It is assumed that the production and consumption will be influenced by market dynamics. Selling and buying electricity also requires the involvement of payment infrastructure. Both the Smart Grid and the payment infrastructure is evolving towards a 5G service-oriented architecture.

By simulating and observing the effects of catastrophic failures in the different infrastructures interdependencies can be identified.

5.2.1 Data Centre Failure

Overall control and implementation of the 5G network centralise risk into the services and core 5G network. A catastrophic failure in the data centres is simulated by increasing the restoration parameter to equal two days of repair time. By studying how this scenario affects the scenario context, we can analyse the impact of such a catastrophic event on a household in the Smart Grid.

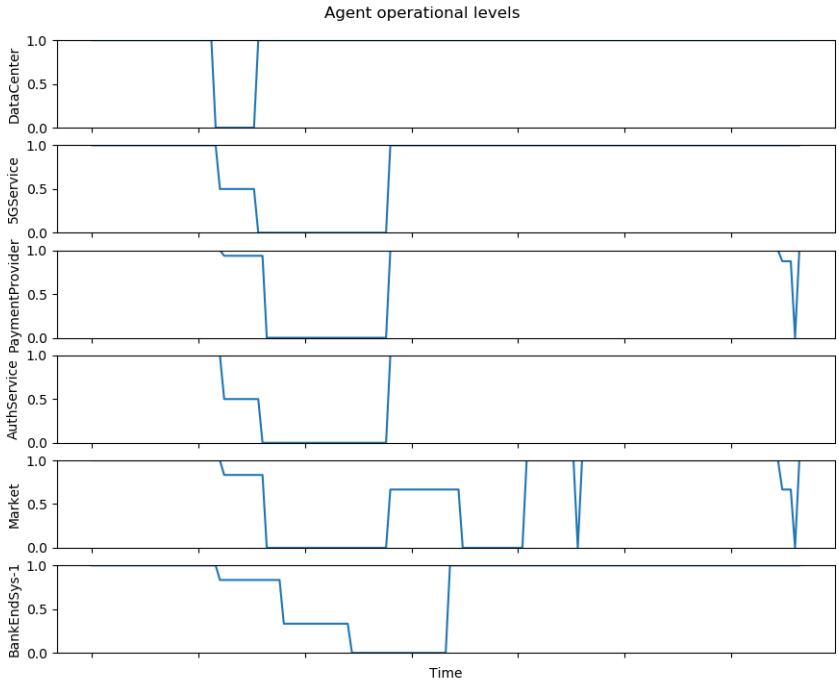

Figure 5.3: Plot of OL for components in the data centre failure, with focus on the propagation of failure in the financial infrastructure.

The from Figures 5.3 and 5.4 we see the catastrophic failure in the data centre propagates trough the infrastructures as illustrated in Figure 5.5.

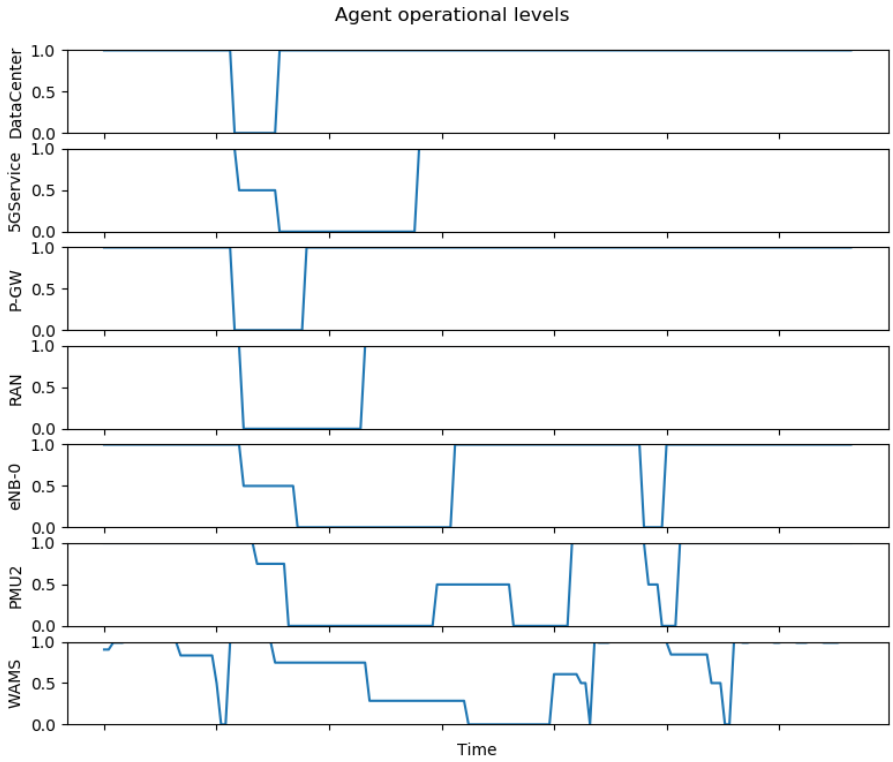

Figure 5.4: Plot of the OL for components in the data centre failure scenario on the propagation of failure in the communication infrastructure.

Discussion

The data centre failure scenario is deemed highly unlikely, but in the event of a data centre failure, the consequences are massive. By studying Figure 5.3 and 5.5, it is clear that a data centre failure would create a failure in the 5G service, which many of the financial infrastructure components rely on. The failure of the authentication service would inhibit the customer's ability to identify themselves for both the commercial banks and the payment providers.

It is reasonable to believe that also the payment providers and commercial bank customer systems (BankEndSys) are directly affected by the 5G service failure. Nevertheless, the commercial bank customer systems experience a prolonged restoration, due to its cyber dependency to the authentication systems. The market also fails as a direct consequence of the 5G failure. However, it is observed that the restoration of the market does not seem as smooth as the other components. It suggests that this

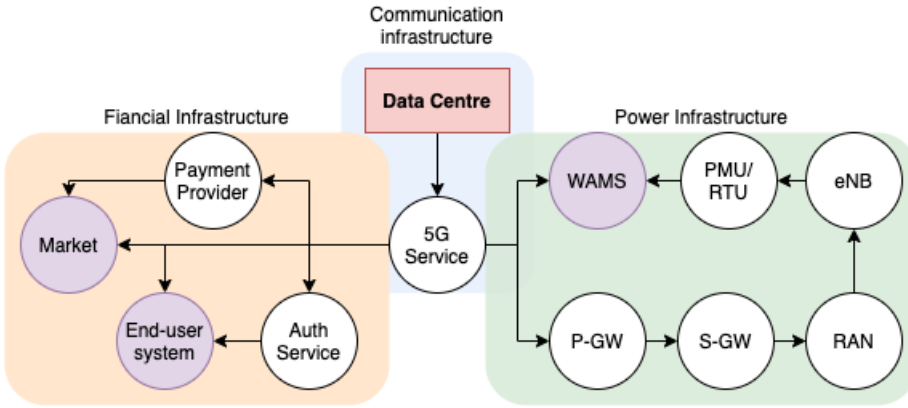

Figure 5.5: Failure propagation from catastrophic failure in the data centre.

prolonged restoration may be caused by an occurrence of a common failure internally or propagating from the power infrastructure.

A failure such as the one in this scenario would with high probability cause significant damage to the market economic dynamics, although these are highly unpredictable. The implications of the financial infrastructure failure in this scenario for a Smart Grid household would imply an inability to perform financial transactions. One could argue that this may not be of critical importance immediately, but with such a failure spanning several days, the failure of the market would create uncertainty in electricity prices which impacts production.

There are similarities in the direct failure of the data centres and the power system infrastructure. However, as illustrated in Figure 5.4, the failure of the 5G service propagates trough the 5G infrastructure failing the P-GW (through the S-GW), RAN and eNBs (illustrated by eNB-0 for simplicity). The failure of 5G service directly impacts the SE abilities of the WAMS, but in the restoration of the 5G service, it can be observed that the WAMS struggles further. As a consequence of the transport network propagation failure, the smaller components of the Smart Grid, the PMUs and the RTUs (illustrated by only PMU2 for simplicity) are failing. This cascading failure results in a delayed restoration of the WAMS SE abilities.

A failure in data centre functionality will result in major cascading failures. This scenario is improbable, and many of the advantages of moving processing and control to data centres are the increased reliability it provides compared to other solutions. The data centres also provide redundancy in their systems, further lowering the probability of complete failure. However, the centralisation of data processing both geographically and virtually creates new interdependencies and challenges. One of

the reasons data centres are efficient is their low amount of staff. In the case of a pandemic where essential staff become affected, a catastrophic failure with a two day reparation period is probable. As illustrated in this scenario, the power and financial infrastructure have a common dependency on the 5G service. A failure of the 5G service is likely to cause cascading failures that will make the restoration of both financial and Smart Grid functionality more challenging.

5.2.2 Central Bank Failure

The second scenario simulates the failure of the central bank, the core component in the financial infrastructure. The central bank component does have a high focus on reliability and security and therefore has a low failure rate. However, a catastrophic failure event could occur concurrently with operational failure. By simulating such a failure event, we can discover cascading effects which contribute to the discussion in Section 2.4.5 surrounding the implementation of DLT in a central bank system.

As with the set up for the data centre failure scenario, the restoration rate of the central bank is increased. The failure rate also increases and will assist in artificially provoke a failure that is extremely unlikely to happen based on the estimated failure rates of the central bank.

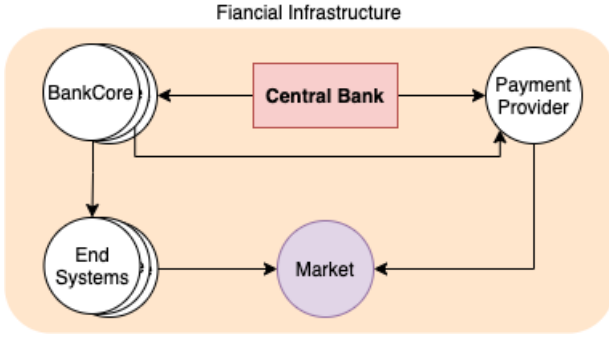

Figure 5.6: Failure propagation route from the catastrophic failure in the central bank scenario.

Based on the subplot in Figure 5.7 we can develop the propagation path illustration seen in Figure 5.6.

Discussion

In the plot of a central bank failure illustrated in Figure 5.7 and 5.6, the direct failures of all dependent components in the infrastructure is imminent. The implications for a Smart Grid household might be more indirect. The ability to perform functions in regards to financial transactions would adhere. As the central bank's functionality is

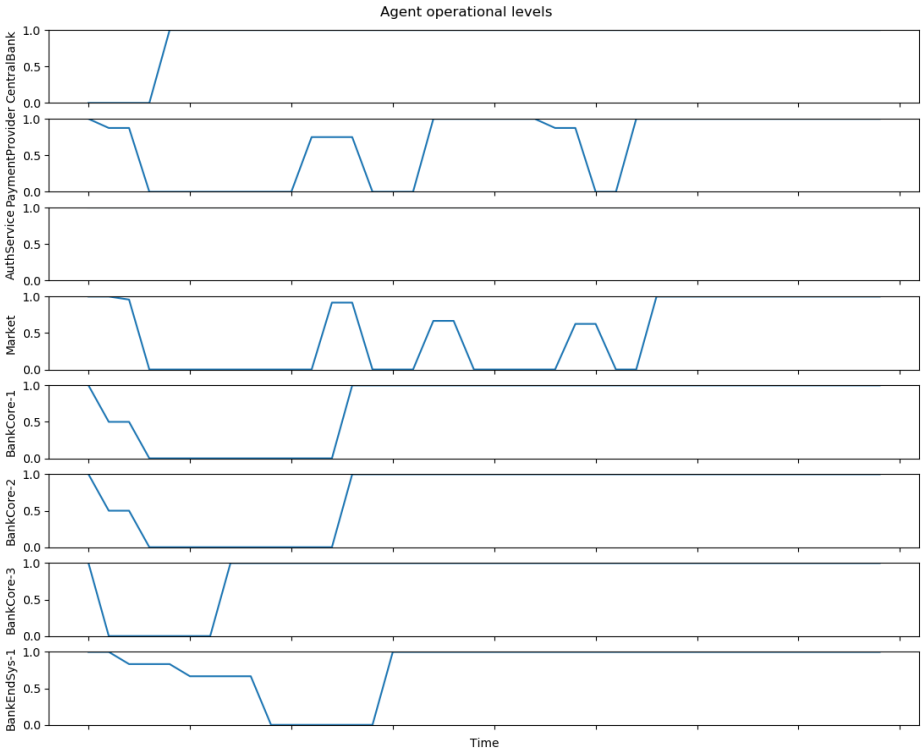

Figure 5.7: Plot of OL for components in the central bank failure scenario. Note that the central bank agent has entered a failure state from the start of the graph. The authentication service is the only financial infrastructure component not effected by the failure.

restored, it can be observed that the cascading effects create a delayed restoration for several components. It can also be argued that the market and payment providers inter-infrastructure dependencies are a factor that develops a prolonged period of instability in the restoration period for both components.

The economic consequences of such a scenario are unpredictable, but there is a high probability that it reveals several logical interdependencies of an economic nature. As seen in the previous analysis of catastrophic events, interdependencies formerly invisible become critical. The consequences for the american financial infrastructure after the 9/11 attacks and the 2008 financial crisis was immense. Such events occurring in the financial infrastructure provides a good example of how economic interdependencies can cascade into global catastrophes, at great speeds.

The simulation result from this scenario can provide an important element in the debate around introducing DLT in the financial infrastructure. The core architecture of the financial infrastructure, which increases the risk of cascading failures by having a centralised ledger system represented by the central bank is demonstrated in the result.

5.2.3 SCADA Failure

A critical component of the power systems is identified as the SCADA controls. Even with the extensive implementation of the Smart Grid, the SCADA control is predicted to still play an essential role in the control and management of the electrical grid. This scenario simulates a catastrophic failure of the SCADA system, which is restored after two days.

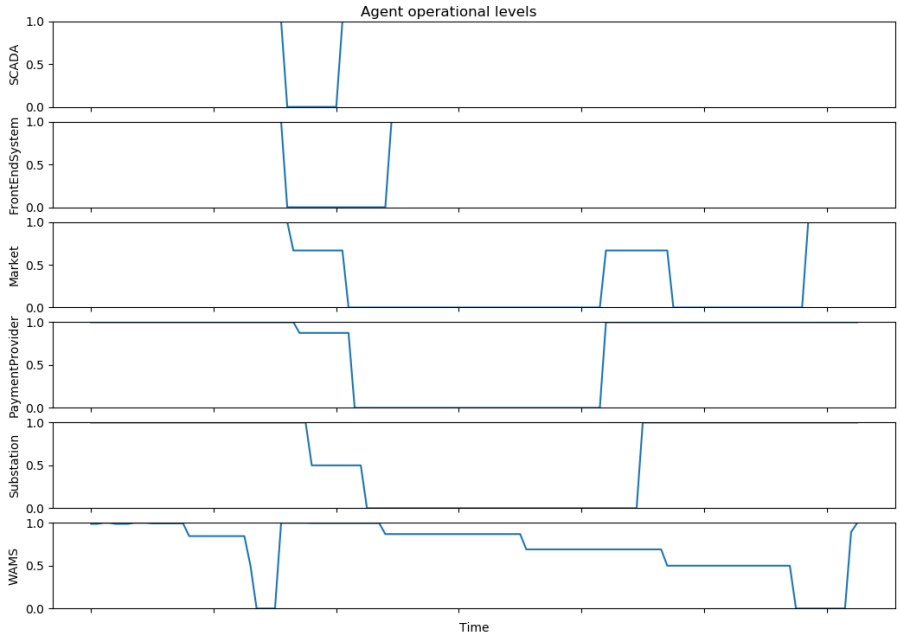

Figure 5.8: Plot of OL for agents in the SCADA failure scenario.

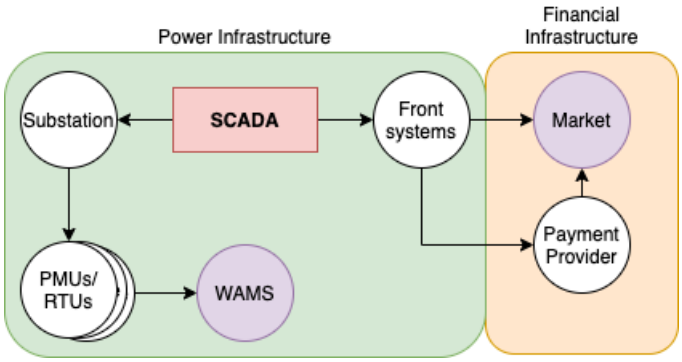

Figure 5.9: Failure propagation route from the catastrophic failure in the SCADA.

Discussion

Out of the three presented failure scenarios, there is reason to believe that a catastrophic failure of SCADA systems is the most probable. Events around the world have shown that SCADA systems in the power infrastructure are a high priority target for hostile entities with the aim of damage [40]. It is, therefore, of high importance to identify and explore the effects and interdependencies surrounding such a failure.

Figures 5.8 and 5.9 reveal a similar pattern to the previous scenarios, the failure quickly escalates to the surrounding subsystems (FrontEndSystem and Substation), and from there creates a cascading failure in market and payment functionality.

Along with the cascading failures experienced by the financial infrastructure, the Smart Grid is experiencing sever functionality failure. The WAMS operational levels are more prone to failure as Figure 5.8 shows, there is reason to believe that the WAMS had recently recovered from a minor escalating failure due to common failure in the PMUs or RTUs. The WAMS is, however, struggling to recover from a cascading failure from the SCADA failure. This failure would create an inability of SE to be performed, which causes an inability for the Smart Grid households to operate.

Chapter 6
Discussion

In this chapter, the relevance and context of the results presented in Chapter 5 is discussed. With a basis in that discussion, the design and implementation issues are presented. Possible additions and solutions are suggested. A central part of this modelling is the knowledge gained by applying the agent-based approach to such a broad scope. This chapter discusses the method and the choice of the modelling approach, including what challenges this poses.

6.1 Future Technologies Create New Interdependencies

The new 5G infrastructure creates broad and unpredictable interdependencies. By studying infrastructure behaviours, it is possible to deduce catastrophic failure scenarios that assist in preparing for emergencies. Simulation of these failure scenarios also reveals new interdependencies.

There are exciting trends in the development of all three infrastructures studied in Chapter 2. The financial and power infrastructures are trending towards a distributed control architecture. Smart Grid technologies use of the 5G network has allowed users to have more control and in many ways, aim to decentralise the power infrastructure. There are signs of similar trends in the financial infrastructure, especially with the emerging DLT. As reviewed in Chapter 2, the DLT will depend on a distributed control which can be enabled by the 5G services and cloud computing. The vulnerability of centralised control systems like the central bank and SCADA have in catastrophic failure events is shown in Chapter 5. Whether a transition to a DLT would mitigate the impact of cascading failure should be investigated further.

However, the 5G evolution is not trending towards an architecture that provides more decentralised control. Even with the introduction of edge cloud computing, the 5G network consists of significant logical and cyber interdependencies with the central 5G core network [19]. There seems to be no trend towards a more distributed control

of the 5G network, and this may create vulnerabilities and increasing interdependence between the financial and power infrastructure.

6.1.1 Corona-crisis and How Catastrophic Events Highlight Infrastructure Interdependence

In early 2020, the world experienced a significant pandemic known as the corona crisis. As with all crisis, the corona crisis exposes how critical a functioning infrastructure is for society. The focus on functions critical to society has highlighted the importance of robust critical infrastructure. In addition to the health services, the critically of government and financial functions has been illustrated.

In a pandemic scenario such as the corona crisis, the most critical aspect and the first to be addressed is the safeguard of human life, thereby implicating the health services. Secondly, the focus quickly shifts to safeguard the economic impact of a societal shutdown. It is essential to consider how an economic recession also impacts health and political stability [12, 59]. The governmental response in regards to stabilising the economy lays the foundation for the length and consequence of how a crisis will impact the economy long term.

It is in the events of necessary government stabilisation of the economy, the importance of a robust, well functioning financial infrastructure become apparent. The dynamics and robustness of the financial institutions like the central bank and commercial core banking systems are generally not discussed. It is with such crisis it becomes evident that a breakdown in the financial infrastructure, lasting hours or days, will have a significant impact on businesses and private individuals. The financial consequences of the corona crisis are also predicted to be long term, party due to cascading failure dynamics, for example, cascading bankruptcies.

A pandemic is an example of a crisis that may threaten the operational and restoration capabilities of the central bank systems. Mainly a pandemic impacting the health of crucial operating personnel in the central bank may render an increased restoration time, as seen in the central bank failure scenario. The result from simulating this scenario gives insight into the markets exposure to such failures. This exposure may be mitigated with local decentralised energy markets which are not influenced by market destabilisation in the same degree and may help to stabilise the power production in the Smart Grid.

6.2 Modelling Challenges

The process of developing an infrastructure interdependence model poses several challenges and issues. In this section, some of the most critical challenges are addressed and discussed.

6.2.1 Design and Implementation Issues

There are several issues which can be considered design and implementation issue occurring in this project.

Simulation time and failure rate management

Not addressing this early in the design and implementation phase develops into a more substantial challenge in analysing results. The time management is fundamental to the accuracy of the simulator and should be planned early in the implementation. There are several approaches to addressing the issue of time management. This simulator the time is related to the system time, in milliseconds, in which ten milliseconds of the system time represents one day of operation in real-time. Literature often presents the component failure rates in hours/days, and can quickly be implemented in the model. However, a different approach would be to implement a separate simulator time as a controlling component of the simulation. Implementing a simulator time enables the simulator to assert a more rigid time frame around the simulation, and also provide more intuitive results for analysis. Issues like simulation time management are also addressed by [14].

Weighed dependencies

Another issue concerning the implementation of this model is the lack of weights of the dependencies. Realising that agents dependencies are weighed equally creates challenges for agents depending on several smaller agents and one larger agent. Taking the WAMS as an example, the functioning of the WAMS logically depends on the workings of most PMUs and RTUs in a Smart Grid, but even more on the 5G services in which the WAMS functionality does most of the State Estimation. In this model, the dependency towards each PMU and RTU was equally as important as the 5G Services dependency, which is a considerable discrepancy in regards to the real-world functioning. In this instance, the issue with the WAMS was fixed by using another middle agent that summarised the PMU and RTU OL before sending it to the WAMS, evening out the dependency weighting sufficiently. This issue does, however, highlight the challenge posed by a varying abstraction level in the model. As mentioned in Section 2.1.4, the model is developed with both low-level abstraction in some parts and higher in others. It can be argued that the issues regarding the

weighted dependencies are present as a result of implementing a solution which can be regarded as a compromise between Panzieri and Porcellinis [47, 48].

6.2.2 Introducing Societal Type Agents

One of the strengths of the agent-based approach is its ability to model social agents. This strength could be applied in this model by introducing different societal agents, representing human and societal behaviour. This would address challenges regarding the implementation of logical interdependencies in the financial infrastructure. It can be argued that the model developed in this thesis is heavily focused on the cyber interdependencies, which are essential in the communication and power infrastructure, but does not capture critical, logical interdependencies in the financial infrastructure. The financial infrastructure is built on societal trust and human resources. These may be considered soft components, but they are significantly crucial in the financial infrastructure, and there is reason to believe that this creates several logical interdependencies for communication and power infrastructures.

The agent-based approach may be suited for introducing such soft components, but this would depend on the accuracy of societal behaviour models, which are hard to validate. Introducing the societal perspective may be more appropriate with a System Dynamic where the abstraction level of the model is significantly higher, and top-down modelling may yield a lower number of components to analyse.

6.2.3 Event Logging

An issue with the model implementation is the simulators inability to produce concentrated information about cascading events. This stems from the implementation tools(JADE) limited evaluation and analysis support. This limitation creates a necessity of visually analysing the results and assume the cause of failures since the agent failures are not logged with the cause of failure. It would be a great advantage to be able to capture cascading failures as events. By doing so, the scenarios could be able easier to assess in a more precise, reliable and quantifiable way.

This issue may have been solved by other implementation tools, but with the JADE environment, it can be solved by implementing a ticket system for each internal agent failure. Assigning this ticket with all escalating failures in the connected agents would better enable the analysis of cascading events, and increase the accuracy and certainty in the result. Enabling this may require a more event focused model, which is necessary to address early in the implementation stage.

6.3 Method and Approach Review

This section discusses the advantages, opportunities and challenges with designing and modelling the three infrastructures using the agent-based approach. The discussion addresses the final objective of this thesis, as presented in Section 2.5.

6.3.1 Model Representativeness

Analysing how accurate the model is in regards to the systems it is meant to represent is a challenging task. The model can be considered both a quantitative and qualitative model. It contains and produces quantitative data for analysis, but also relies on qualitative behaviour descriptions and assumptions. These perspectives have an impact on model representativeness. Narrowing the simulation scope with introducing an initial case increases the model accuracy. At the same time, modelling three infrastructures in one model is to be considered a wide scope.

Varying abstraction levels

The variation in the level of abstraction in the model poses more considerable challenges than initially expected. One of the advantages of the agent-based approach is the support for flexibility and heterogeneity in subsystem components. However, the difference in abstraction level designed in this model stretches the possibilities far. In Chapter 4, the estimations and approximations to develop the agents of the financial system may be considered as less accurate than for the components in the Smart Grid. This difference in accuracy is contributed to the difference in abstraction level.

Data collection challenges

The underlying uncertainty of modelling systems still in development is a challenge which does affect the accuracy of the model. To mitigate this uncertainty, assumptions and generalisations about the 5G and the Smart Grid are made. The system assumptions and behaviour estimations are based on former models, studies and white papers, which provide a degree of accuracy and certainty.

In modelling the 5G, the background is mostly provided by requirements based on common use cases developed by the 3GPP [20]. This data background allows for a certain amount of uncertainty and inaccuracy. However, this is mitigated by minimising the amount of functionality addressed by the agents in the model. The amount of proposed models and architectures of the 5G makes the modelling challenges and may decrease the accuracy of the model.

Smart Grid architecture is well explored as seen in Section 2.3.2, and some well-established models describe and simulate this infrastructure which provides this

model with reliable and detailed sources for the background. Simplifications are also made in regards to the Smart Grid part of the model. However, the assumptions and simplifications made in this domain have a more reliable basis in previous modelling research than the financial and communications infrastructures, for reasons that have been previously discussed.

The model of the financial infrastructure is challenging due to its difference in each currency zone and country. While some infrastructures like the U.S still rely on the use of banking checks, other financial infrastructures have completely disregarded both checks and cash to some degree. This creates considerable differences in the importance of the digital payment providers, central bank, authentication systems, which in turn impacts the qualitative assumptions of the component behaviours.

6.3.2 Large Model Scope Using Agent-based Modelling Approach

Based on the systematic review of literature on modelling interdependencies in Section 3.2, a plan for the model development was created. Deciding on using the agent-based approach set a framework for the model design and implementation, even though agent-based modelling is one of the more flexible approaches to modelling, there are still challenges in using this approach.

Little research is done on agent-based modelling with the scope of three infrastructures. As with this model, a challenge with a bottom-up approach with such a wide scope is the required insight necessary to produce an accurate agent and behaviour description. Creating a model with sufficient detail in behaviour and communication is challenging and time-consuming. This modelling shows that applying the agent-based approach on a case spanning three infrastructures pushes the limits of appropriateness. The number of components identified in this model is large compared to other agent-based models. As a consequence, the number of estimations, approximations, and compromises necessary in the agent development is high and makes room for more uncertain.

Using a more holistic approach, like the SD or IIM approaches presented in Section 3.2 might have increased the ability to provide more quantitative results, however with lower accuracy and less granularity. Not being able to identify how subsystems behave and communicate across the infrastructures would probably inhibit the ability to analyse what subsystems are vulnerable in the modelling scenarios.

In addition to the implementation issues discussed in the above section, a stricter limitation in the scope of the model may increase its accuracy and capability of producing quantitative results.

Chapter 7
Conclusion

This thesis explored the field of modelling interdependencies in critical infrastructure by answering the question of what interdependencies may develop between the financial, communications and power infrastructures in the migration towards 5G and Smart Grid future. This question is rooted in the case of households becoming both producers and consumers in the electricity infrastructure and wanting to perform financial transaction based on this production and consumption. With a basis in this initial case, the first objective is met by achieving an understanding of the financial, communications, and power infrastructure. In Chapter 2, a theoretical basis of the interdependency modelling field is presented. The core architecture and the functionalities required from the different infrastructures in regards to the case are explored. This exploration provides a base to the model design by discovering how the infrastructures are interconnected.

The second objective of this thesis is to analyse which modelling approach is most appropriate for this modelling task. Even though interdependency modelling is a relatively immature field; there are several different approaches relevant for this type of modelling. In Chapter 3, several approaches are explored and discussed, and the agent-based approach is deemed the most suited approach for this modelling. The agent-based approach supports a flexible abstraction level in the model and its maturity in regards to the available modelling tools. After a tool analysis, the JADE-tool is selected as the modelling tool.

With the agent-based approach selected, the model is designed and implemented. As presented in Chapter 4, the model design is developed by exploring the necessary functionality for the case in each subsystem, and minimising the number of components in the model. At the same time, uphold a level of granularity to identify interdependencies in the subsystems. By building upon the research performed in Chapter 2, the model components are identified. Using UML, the model is drawn with several steps.

After the model implementation, simulations are performed on the model in a reliability sense. The simulation results identify that the market component is vulnerable and suffers from a lower ability to perform due to interdependencies. It is identified that several internal failures in all three infrastructures escalate or cascades to affect the market component. Therefore it is arguable a highly exposed component in the infrastructure system. How failure in the market component affects societal aspects and the households in the Smart Grid is also discussed.

By developing different scenarios, the model is used to explore infrastructure behaviours in catastrophic failure events. It finds that a catastrophic failure of the data centres creates massive cascading failures in all three infrastructures. In trying to restore to operational functions, interdependencies cascading in the 5G infrastructure may inhibit the fast recovery of the essential Smart Grid functionality. The second scenario identifies that central bank failure has both economic and technical consequences that are challenging to predict. It is debatable how the financial infrastructures core architecture may be a technically vulnerable solution, and the DLT may be proposed as an alternative solution to increase reliability in this infrastructure system.

The introduction of 5G promises several improvements to reliability, as well as revolutionising services that can enable a new generation of technology development. One of the early developments is the Smart Grid, and with this model, it serves as an example of how the 5G evolution develops more interdependencies in the infrastructure systems. The 5G shift also enables more systems to implement decentralised control, while the 5G itself proposes a centralised control architecture. This shift in control may cause a false sense of security, in that services like the Smart Grid find security in its decentralised control, while relying heavily on a centralised 5G service.

In Chapter 6, the issues regarding the model design and implementation are presented. The solution to these issues is discussed and proposed. This discussion provides a summation of knowledge and experience gathered through the modelling process. Since the agent approach is rarely used for modelling infrastructure systems of this scope, the modelling approach decision is discussed in regards to the modelling decisions and results. The discussion explores the advantages and challenges in applying such non-holistic approaches to more than two infrastructures.

There is an overall development towards more interconnected infrastructures, and even though the 5G shift development poses several challenges in both modelling and predicting cascading failures, it may also enable more robust infrastructures. The final chapter of this thesis proposes additional modelling features and challenges that may be addressed to provide more in-depth insight into the field of interdependence modelling.

Chapter 8
Future work

In this chapter, additional functionality for the model is proposed and further development of the model to explore other scenarios that are predicted to become relevant.

8.1 Additional Features for the Model Design and Implementation

In future work to improve the accuracy of this model and simulation, several features would be appropriate:

- Introducing social agents and model societal responses to infrastructure failure, as explained in Section 6.2.2. Starting with the introduction of agents with behaviour based on economic models may develop interesting results both for infrastructure interdependence research and economic predictions.

- Include multiple failure modes to increase accuracy. These failure modes, as suggested in Panzieris 2004 paper, comprise of different failure types within each agent, and each failure type had different restoration time [47]. This would naturally induce several scenarios and create a more granulated simulation.

- Expanding the model to include resilience dependencies. This would entail that after an agent failure, other dependencies than those required in the normal operations, are required. Along with implementing different failure types, the agents could be dependant on different agents for restoring different failure types. For example, physical failure of an eNB would require manual reparation, represented by a different dependency than a minor software crash which would demand a virtual restart.

8.2 Future Modelling Challenges

Several technical advances mentioned in Chapter 2 proposes valuable modelling challenges. The ones with the highest probability of being implemented in the near future would be the DLT and 5G services.

8.2.1 Distributed Ledger Technology

As explored in Section 2.4.5 DLT is a popular and well discussed technical solution within the financial infrastructure domain. However, what interdependencies this transition would create is not explored in a broad context. Developing a model which studies the consequences of a more distributed financial infrastructure could reveal arguments for and against such a transition, and would give valuable knowledge in the technical implementation of a DLT solution.

8.2.2 Granulation of 5G Services

With a basis in the model created in this thesis, granulation of the 5G services may identify new interdependencies within the three modelled infrastructures. As mentioned in the background research, the 5G service is comprehensive and somewhat undefined and therefore challenging to model. However, such complex systems often develop into ticking time bombs of interdependencies. It would, therefore, be essential to identify the cyber interdependencies inside the 5G services and include how the different parts of the Smart Grid rely on different 5G services.

References

[1] Sameera Abar, Georgios K. Theodoropoulos, Pierre Lemarinier, and Gregory M. P. O'Hare. 2017. Agent Based Modelling and Simulation tools: A review of the state-of-art software. *Computer Science Review* 24 (May 2017), 13–33. https://doi.org/10.1016/j.cosrev.2017.03.001

[2] Azamat Abdymomunov, Filippo Curti, and Atanas Mihov. 2020. U.S. Banking Sector Operational Losses and the Macroeconomic Environment. *Journal of Money, Credit and Banking* 52, 1 (2020), 115–144. https://doi.org/10.1111/jmcb.12661 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/jmcb.12661.

[3] Mamta Agiwal, Abhishek Roy, and Navrati Saxena. 2016. Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys Tutorials* 18, 3 (2016), 1617–1655. https://doi.org/10.1109/COMST.2016.2532458 Conference Name: IEEE Communications Surveys Tutorials.

[4] Ijaz Ahmad, Tanesh Kumar, Madhusanka Liyanage, Jude Okwuibe, Mika Yliant-tila, and Andrei Gurtov. 2018. Overview of 5G Security Challenges and Solutions. *IEEE Communications Standards Magazine* 2, 1 (March 2018), 36–43. https://doi.org/10.1109/MCOMSTD.2018.1700063 Conference Name: IEEE Communications Standards Magazine.

[5] Iñaki Aldasoro, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach. 2020. *Operational and Cyber Risks in the Financial Sector*. SSRN Scholarly Paper ID 3549526. Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=3549526

[6] NGMN Alliance. 2016. Description of network slicing concept. *NGMN 5G P* 1 (2016), 1.

[7] Almende. 2020. Eve - Introduction. https://eve.almende.com/index.html

[8] Freek Baalbergen, Madeleine Gibescu, and Lou van der Sluis. 2009. Modern state estimation methods in power systems. In *2009 IEEE/PES Power Systems Conference and Exposition*. 1–6. https://doi.org/10.1109/PSCE.2009.4840003

[9] J. Bartelt, N. Vucic, D. Camps-Mur, E. Garcia-Villegas, I. Demirkol, A. Fehske, M. Grieger, A. Tzanakaki, J. Gutiérrez, E. Grass, G. Lyberopoulos, and G. Fettweis.

2017. 5G transport network requirements for the next generation fronthaul interface. *EURASIP Journal on Wireless Communications and Networking* 2017, 1 (May 2017), 89. https://doi.org/10.1186/s13638-017-0874-7

[10] Morten L. Bech and Rodney Garratt. 2017. *Central Bank Cryptocurrencies*. SSRN Scholarly Paper ID 3041906. Social Science Research Network, Rochester, NY. https://papers.ssrn.com/abstract=3041906

[11] Fabio Bellifemine, Agostino Poggi, and Giovanni Rimassa. 1999. JADE–A FIPA-compliant agent framework. In *Proceedings of PAAM*, Vol. 99. London, 33. Issue: 97-108.

[12] Stephen Bezruchka. 2009. The effect of economic recession on population health. *Cmaj* 181, 5 (2009), 281–285. Publisher: Can Med Assoc.

[13] A. Bobbio, E. Ciancamerla, S. Di Blasi, A. Iacomini, F. Mari, I. Melatti, M. Minichino, A. Scarlatti, E. Tronci, R. Terruggia, and E. Zendri. 2009. Risk analysis via heterogeneous models of SCADA interconnecting Power Grids and Telco networks. In *2009 Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS 2009)*. 90–97. https://doi.org/10.1109/CRISIS.2009.5411974 ISSN: 2151-4763.

[14] Emiliano Casalicchio, Emanuele Galli, and Salvatore Tucci. 2007. Federated Agent-based Modeling and Simulation Approach to Study Interdependencies in IT Critical Infrastructures. In *11th IEEE International Symposium on Distributed Simulation and Real-Time Applications (DS-RT'07)*. 182–189. https://doi.org/10.1109/DS-RT.2007.11 ISSN: 1550-6525.

[15] Aleksandra Checko, Henrik L. Christiansen, Ying Yan, Lara Scolari, Georgios Kardaras, Michael S. Berger, and Lars Dittmann. 2015. Cloud RAN for Mobile Networks—A Technology Overview. *IEEE Communications Surveys Tutorials* 17, 1 (2015), 405–426. https://doi.org/10.1109/COMST.2014.2355255 Conference Name: IEEE Communications Surveys Tutorials.

[16] Gabriel J. Correa-Henao, Jose M. Yusta, and Roberto Lacal-Arántegui. 2013. Using interconnected risk maps to assess the threats faced by electricity infrastructures. *International Journal of Critical Infrastructure Protection* 6, 3 (Dec. 2013), 197–216. https://doi.org/10.1016/j.ijcip.2013.10.002

[17] Mounaim Cortet, Tom Rijks, and Shikko Nijland. 2016. PSD2: The digital transformation accelerator for banks. *Journal of Payments Strategy & Systems* 10, 1 (2016), 13–27. Publisher: Henry Stewart Publications.

[18] Mirsad Cosovic, Achilleas Tsitsimelis, Dejan Vukobratovic, Javier Matamoros, and Carles Anton-Haro. 2017. 5G Mobile Cellular Networks: Enabling Distributed State Estimation for Smart Grids. *IEEE Communications Magazine* 55, 10 (Oct. 2017), 62–69. https://doi.org/10.1109/MCOM.2017.1700155 Conference Name: IEEE Communications Magazine.

[19] Roger Gary Cox, Dianne Catherine Barton, Rhonda K. Reinert, Eric D. Eidson, and David Alan Schoenwald. 2004. *Simulating economic effects of disruptions in the telecommunications infrastructure.* Technical Report SAND2004-0101, 918354. SAND2004–0101, 918354 pages. https://doi.org/10.2172/918354

[20] Philipp Deibert. [n.d.]. *NGMN 5G White Paper (Accessed: 25.11.2019).* Technical Report. NGMN Alliance. 125 pages. https://www.ngmn.org/wp-content/uploads/NGMN_5G_White_Paper_V1_0.pdf

[21] Bendik Balstad Deraas. 2019. Identifying interdependencies in critical infrastructure. (2019), 15.

[22] Simon Dredge. 2020. What is the 5G Access and Mobility Management Function (AMF)? https://www.metaswitch.com/knowledge-center/reference/what-is-the-5g-access-and-mobility-management-function-amf Library Catalog: www.metaswitch.com.

[23] Uwe Dötsch, Mark Doll, Hans-Peter Mayer, Frank Schaich, Jonathan Segel, and Philippe Sehier. 2013. Quantitative analysis of split base station processing and determination of advantageous architectures for LTE. *Bell Labs Technical Journal* 18, 1 (June 2013), 105–128. https://doi.org/10.1002/bltj.21595 Conference Name: Bell Labs Technical Journal.

[24] Ericsson. 2020. Network architecture functional and physical domains. https://www.ericsson.com/en/future-technologies/architecture/network-architecture-domains Last Modified: 2020-02-18T07:05:56+00:00 Library Catalog: www.ericsson.com.

[25] Jose Oscar Fajardo, Fidel Liberal, Ioannis Giannoulakis, Emmanouil Kafetzakis, Vincenzo Pii, Irena Trajkovska, Thomas Michael Bohnert, Leonardo Goratti, Roberto Riggio, Javier Garcia Lloreda, Pouria Sayyad Khodashenas, Michele Paolino, Pavel Bliznakov, Jordi Perez-Romero, Claudio Meani, Ioannis Chochliouros, and Maria Belesioti. 2016. Introducing Mobile Edge Computing Capabilities through Distributed 5G Cloud Enabled Small Cells. *Mobile Networks and Applications* 21, 4 (Aug. 2016), 564–574. https://doi.org/10.1007/s11036-016-0752-2

[26] K Foit, Waclaw Banas, Aleksander Gwiazda, and P Hryniewicz. 2017. The comparison of the use of holonic and agent-based methods in modelling of manufacturing systems. *IOP Conference Series: Materials Science and Engineering* 227 (Aug. 2017), 012046. https://doi.org/10.1088/1757-899X/227/1/012046

[27] Christopher Guindon. 2020. Eclipse desktop & web IDEs | The Eclipse Foundation. https://www.eclipse.org/ide/ Library Catalog: www.eclipse.org.

[28] O. Gursesli and A.A. Desrochers. 2003. Modeling infrastructure interdependencies using Petri nets. In *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme - System Security and Assurance (Cat. No.03CH37483)*, Vol. 2. 1506–1512 vol.2. https://doi.org/10.1109/ICSMC.2003.1244625 ISSN: 1062-922X.

[29] Yacov Y Haimes and Pu Jiang. 2001. Leontief-based model of risk in complex interconnected infrastructures. *Journal of Infrastructure systems* 7, 1 (2001), 1–12. Publisher: American Society of Civil Engineers.

[30] Gregor Heinrich. 2006. Operational risk, payments, payment systems, and implementation of Basel II in Latin America : recent developments. (2006), 20.

[31] Santander Innoventures and Oliver Wyman. 2015. The Fintech 2.0 Paper: rebooting financial services. *Recuperado de: http://santanderinnoventures. com/wpcontent/uploads/2015/06/The-Fintech-2-0-Paper. pdf* (2015).

[32] Jason. 2020. Description | Jason. http://jason.sourceforge.net/wp/description/ Library Catalog: jason.sourceforge.net.

[33] Sami Kekki, Walter Featherstone, Yonggang Fang, Pekka Kuure, Alice Li, Anurag Ranjan, Debashish Purkayastha, Feng Jiangping, Danny Frydman, Gianluca Verin, and others. 2018. MEC in 5G networks. *ETSI white paper* 28 (2018), 1–28.

[34] Karry Lai. 2018. Singapore banks using DLT to tackle money laundering. *International Financial Law Review* (March 2018). https://search.proquest.com/docview/2032321542?accountid=12870 ISBN: 02626969.

[35] Peter Legg, Gao Hui, and Johan Johansson. 2010. A Simulation Study of LTE Intra-Frequency Handover Performance. In *2010 IEEE 72nd Vehicular Technology Conference - Fall*. 1–5. https://doi.org/10.1109/VETECF.2010.5594477 ISSN: 1090-3038.

[36] Zhi Lü, Yi Lü, Mingzhe Yuan, and Zhongfeng Wang. 2017. A heterogeneous large-scale parallel SCADA/DCS architecture in 5G OGCE. In *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*. 1–7. https://doi.org/10.1109/CISP-BMEI.2017.8302294 ISSN: null.

[37] MaDKit. 2020. MaDKit. http://www.madkit.org/

[38] Dania Marabissi, Lorenzo Mucchi, Romano Fantacci, Maria Rita Spada, Fabio Massimiani, Andrea Fratini, Giorgio Cau, Jia Yunpeng, and Lucio Fedele. 2019. A Real Case of Implementation of the Future 5G City. *Future Internet* 11, 1 (Jan. 2019), 4. https://doi.org/10.3390/fi11010004

[39] Esther Mengelkamp, Benedikt Notheisen, Carolin Beer, David Dauer, and Christof Weinhardt. 2018. A blockchain-based smart grid: towards sustainable local energy markets. *Computer Science - Research and Development* 33, 1 (Feb. 2018), 207–214. https://doi.org/10.1007/s00450-017-0360-9

[40] Bill Miller and Dale Rowe. 2012. A survey SCADA of and critical infrastructure incidents. In *Proceedings of the 1st Annual conference on Research in information technology (RIIT '12)*. Association for Computing Machinery, Calgary, Alberta, Canada, 51–56. https://doi.org/10.1145/2380790.2380805

[41] Marco Moscadelli. 2004. *The Modelling of Operational Risk: Experience with the Analysis of the Data Collected by the Basel Committee*. SSRN Scholarly Paper ID 557214. Social Science Research Network, Rochester, NY. https://doi.org/10.2139/ssrn.557214

[42] Alan T. Murray and Tony H. Grubesic. 2007. Overview of Reliability and Vulnerability in Critical Infrastructure. In *Critical Infrastructure: Reliability and Vulnerability*, Alan T. Murray and Tony H. Grubesic (Eds.). Springer, Berlin, Heidelberg, 1–8. https://doi.org/10.1007/978-3-540-68056-7_1

[43] Tuan Anh Nguyen, Dong Seong Kim, and Jong Sou Park. 2016. Availability modeling and analysis of a data center for disaster tolerance. *Future Generation Computer Systems* 56 (March 2016), 27–50. https://doi.org/10.1016/j.future.2015.08.017

[44] Gabriele Oliva and Roberto Setola. 2015. Infrastructure Interdependencies: Modeling and Analysis. In *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, Elias Kyriakides and Marios Polycarpou (Eds.). Springer, Berlin, Heidelberg, 239–261. https://doi.org/10.1007/978-3-662-44160-2_9

[45] Alexander Outkin, Silvio Flaim, Andy Seirp, and Julia Gavrilov. 2008. FinSim: A Framework for Modeling Financial System Interdependencies. *Applications of Complex Adaptive Systems* (2008), 257–277. https://doi.org/10.4018/978-1-59904-962-5.ch010

[46] Min Ouyang. 2014. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety* 121 (Jan. 2014), 43–60. https://doi.org/10.1016/j.ress.2013.06.040

[47] S. Panzieri, R. Setola, and G. Ulivi. 2004. *An Agent Based Simulator for Critical Interdependent Infrastructures*.

[48] Stefano Porcellinis, Roberto Setola, Stefano Panzieri, and Giovanni Ulivi. 2008. Simulation of heterogeneous and interdependent critical infrastructures. *IJCIS* 4 (Jan. 2008), 110–128. https://doi.org/10.1504/IJCIS.2008.016095

[49] Hafiz Abdur Rahman, Konstantin Beznosov, and Jose R. Marti. 2009. Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. *International Journal of Critical Infrastructures* 5, 3 (2009), 220. https://doi.org/10.1504/IJCIS.2009.024872

[50] S. M. Rinaldi. 2004. Modeling and simulating critical infrastructures and their interdependencies. In *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*. 8 pp.–. https://doi.org/10.1109/HICSS.2004.1265180

[51] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21, 6 (Dec. 2001), 11–25. https://doi.org/10.1109/37.969131

[52] Tony Saboorian and Amanda Xiang. 2017. Network Slicing and 3GPP Service and Systems Aspects (SA) Standard - IEEE Software Defined Networks. (Jan. 2017). https://sdn.ieee.org/newsletter/december-2017/network-slicing-and-3gpp-service-and-systems-aspects-sa-standard Library Catalog: sdn.ieee.org.

[53] Susan V Scott and Markos Zachariadis. 2012. Origins and development of SWIFT, 1973–2009. *Business History* 54, 3 (2012), 462–482. Publisher: Taylor & Francis.

[54] Jan Smets. 2016. Fintech and central banks. In *Conferencia en el Colloquium of the Belgian Financial Forum en cooperación con SUERF, el European Money and Finance Forum y Eggsplore (9 de diciembre)*.

[55] Telecomitalia. 2020. Jade Site | Java Agent DEvelopment Framework. https://jade.tilab.com/

[56] 3GPP TS 23.501. 2015. System Architecture for the 5G System; Stage 2. (2015).

[57] Samuel Tweneboah-Koduah and William J. Buchanan. 2018. Security Risk Assessment of Critical Infrastructure Systems: A Comparative Study. *Comput. J.* 61, 9 (Sept. 2018), 1389–1406. https://doi.org/10.1093/comjnl/bxy002

[58] Uptime Institute. 2020. Data Center Certification: Tier Performance Certification. https://uptimeinstitute.com/tier-certification Library Catalog: uptimeinstitute.com.

[59] Patrick FA Van Erkel and Tom WG Van Der Meer. 2016. Macroeconomic performance, political trust and the Great Recession: A multilevel analysis of the effects of within-country fluctuations in macroeconomic performance on political trust in 15 EU countries, 1999–2011. *European Journal of Political Research* 55, 1 (2016), 177–197. Publisher: Wiley Online Library.

[60] Yang Wang, Wenyuan Li, and Jiping Lu. 2009. Reliability analysis of phasor measurement unit using hierarchical Markov modeling. *Electric Power Components and Systems* 37, 5 (2009), 517–532. Publisher: Taylor & Francis.

[61] Yang Wang, Wenyuan Li, and Jiping Lu. 2010. Reliability Analysis of Wide-Area Measurement System. *IEEE Transactions on Power Delivery* 25, 3 (July 2010), 1483–1491. https://doi.org/10.1109/TPWRD.2010.2041797 Conference Name: IEEE Transactions on Power Delivery.

[62] Wikipedia. 2020. 5G network slicing. https://en.wikipedia.org/w/index.php?title=5G_network_slicing&oldid=949380422 Page Version ID: 949380422.

[63] Wikipedia. 2020. Comparison of agent-based modeling software. https://en.wikipedia.org/w/index.php?title=Comparison_of_agent-based_modeling_software&oldid=939548768 Page Version ID: 939548768.

[64] Athol Yates. 2014. A framework for studying mortality arising from critical infrastructure loss. *International Journal of Critical Infrastructure Protection* 7, 2 (June 2014), 100–111. https://doi.org/10.1016/j.ijcip.2014.04.002

[65] Aldo A Zagonel and Thomas F Corbet. 2006. Levels of confidence in System dynamics modeling: a pragmatic approach to assessment of dynamic models. In *24th International Conference of the System Dynamics Society. Nijmegen, The Netherlands. http://www. systemdynamics. org/conferences/2006/proceed/papers/ZAGON374. pdf.*

[66] Gulnara Zhabelova and Valeriy Vyatkin. 2012. Multiagent Smart Grid Automation Architecture Based on IEC 61850/61499 Intelligent Logical Nodes. *IEEE Transactions on Industrial Electronics* 59, 5 (May 2012), 2351–2362. https://doi.org/10.1109/TIE.2011.2167891 Conference Name: IEEE Transactions on Industrial Electronics.

Appendix A

Appendices

A.1 Simulation Results

A.1.1 Steady State Simulation

Figures A.1-A.4 show the results of the steady state simulation in different time increments. We see that there are minimal differences in the results, and they are coherent.

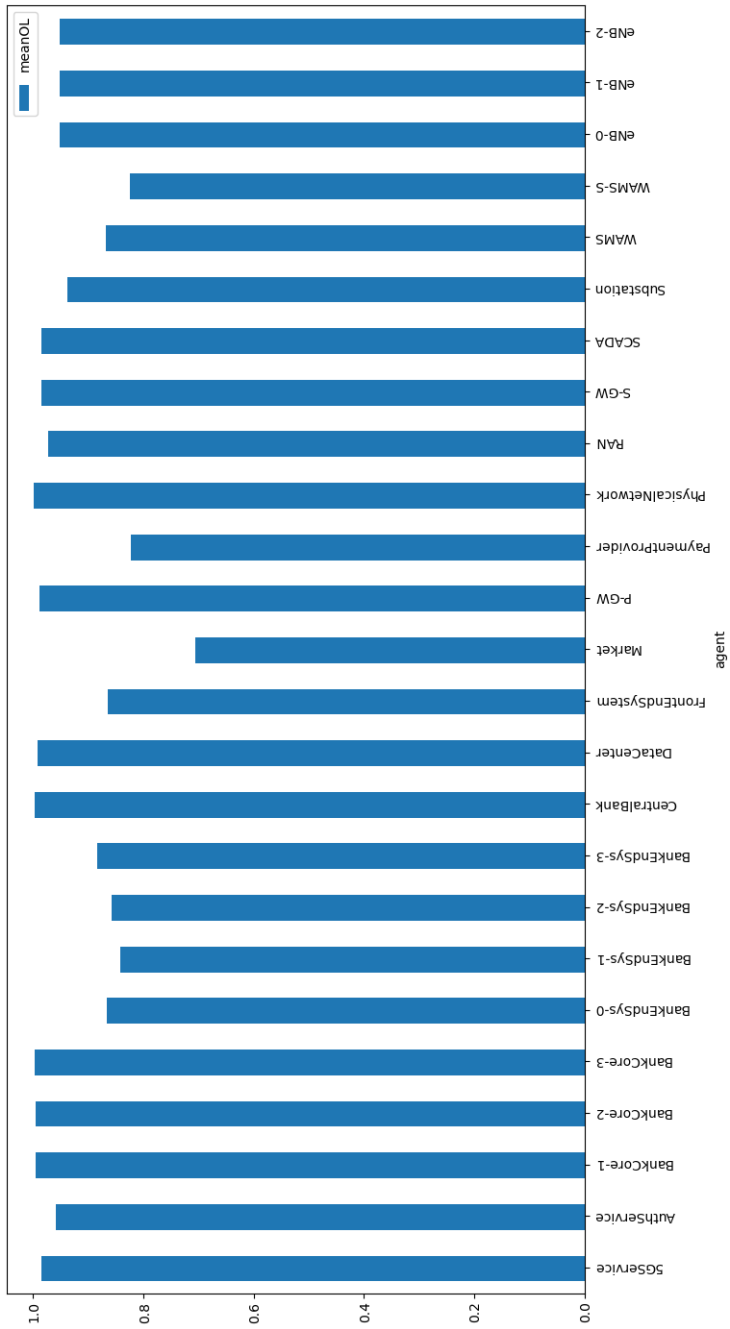

Figure A.1: Mean OL of system run approx. 700years.

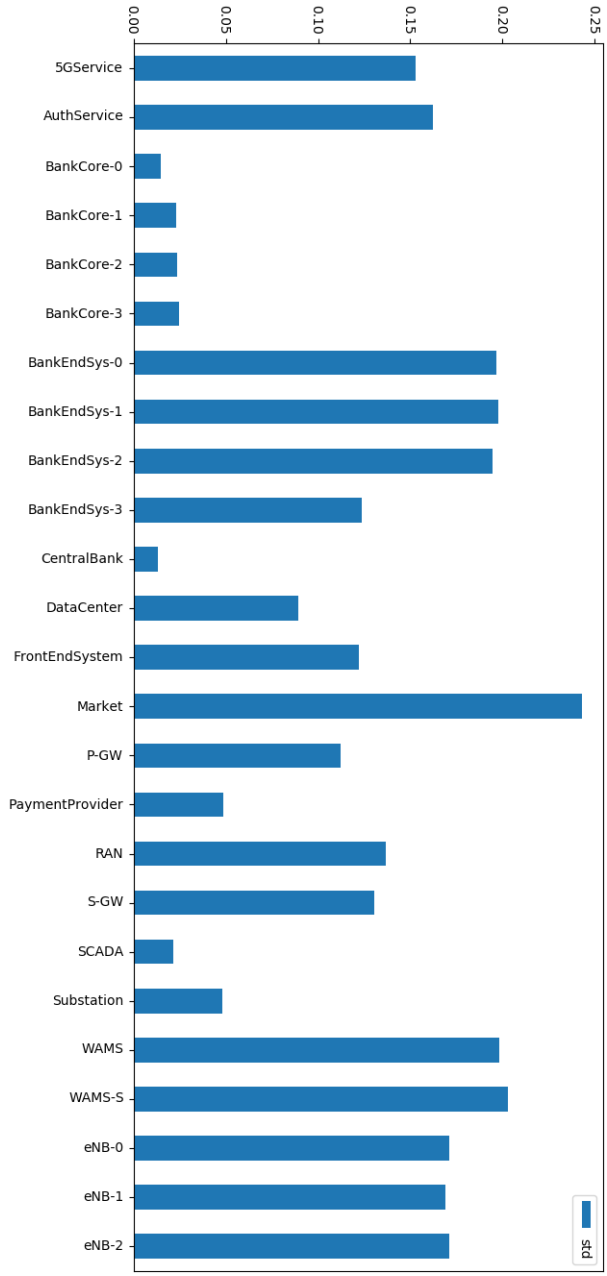

Figure A.2: STD of the agents in a simulation of approx. 700years.

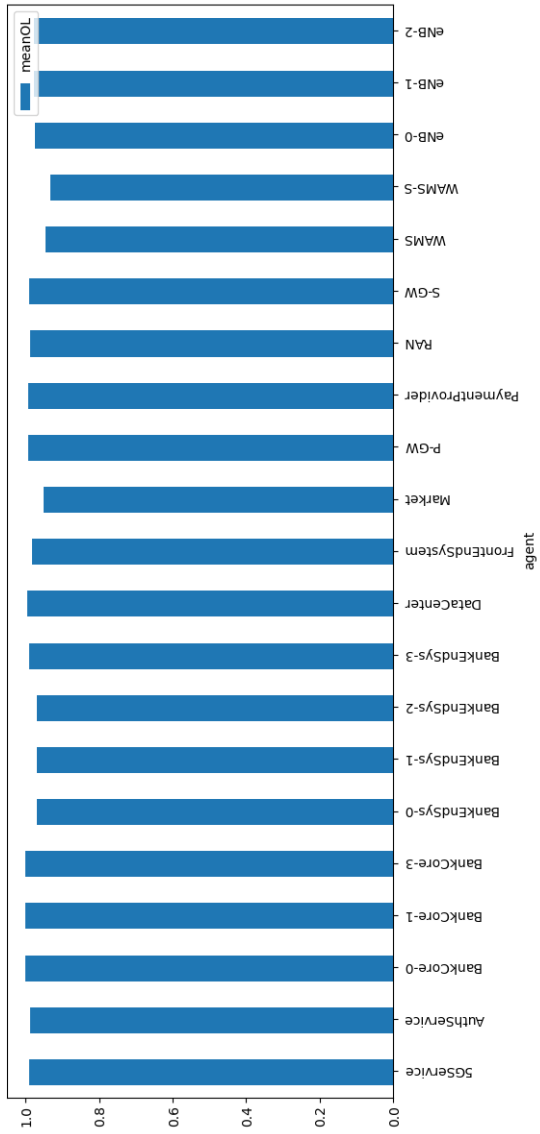

Figure A.3: Mean OL of system run approx. 2000 years.

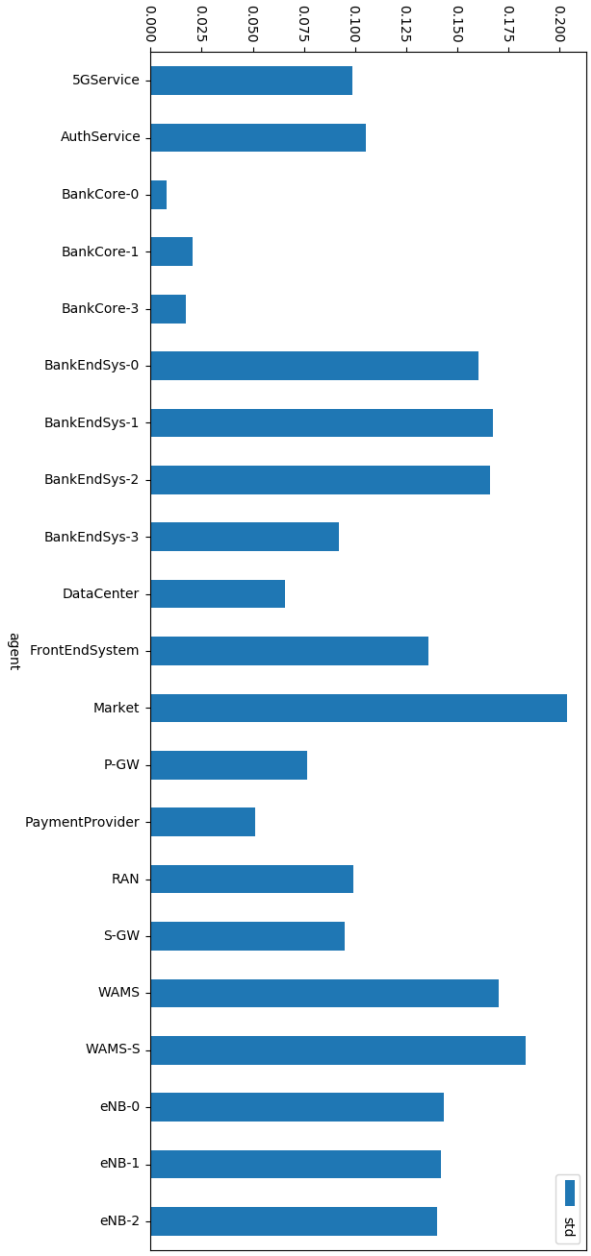

Figure A.4: STD of the agents in a simulation of approx. 2000 years.

Function	Description
Mobility Management Entity (MME)	is the key control function in the EPC network. The main functionality of the MME is attach and detach of UE, authentication, choosing SGW and PGW for the UE, and management of PDN connections and EPC bearers. It also handles mobility procedures, UE tracking, and paging.
PDN Gateway (PGW)	is the gateway between the internal EPC network and external PDNs, for example, the Internet or a corporate LAN. The PGW provides IP connectivity towards external PDNs, policy and admission control, and packet filtering per user. The PGW can also be used for charging.
Serving Gateway (SGW)	routes and forwards the user packet data from the UE to the PGW or from the PGW to the UE. The SGW acts as a local mobility anchor for the user plane during inter-eNodeB handovers and provides charging functionality.
Policy and Charging Rules Functions (PCRF)	handles policy control decisions and flow-based charging control functionality. The main functionality is to evaluate operator policies that are triggered by events received from various functions and to provide rules for application and service data flow detection, gating, QoS and flow-based charging.
Home Subscriber Server (HSS)	is a central database that contains user-related and subscription-related information. The functions of the HSS include functionalities such as storage of the long-term security credentials, subscriber profiles, access authorisation, mobility management support.
Service Capability Exposure Function (SCEF)	is used to securely expose the services and capabilities provided by 3GPP network interfaces. The functionality is brought to 3GPP for standardisation through a function called Application Network Interaction Function (ANIF).
User Plane (UP)	includes e.g. functionality for mobility anchor point, external PDU session point of interconnect, packet routing and forwarding, QoS handling for user plane, packet inspection and policy enforcement lawful intercept.

Table A.1: 5G Core sub-functions [24]

A.2 5G infrastructure sub-functions

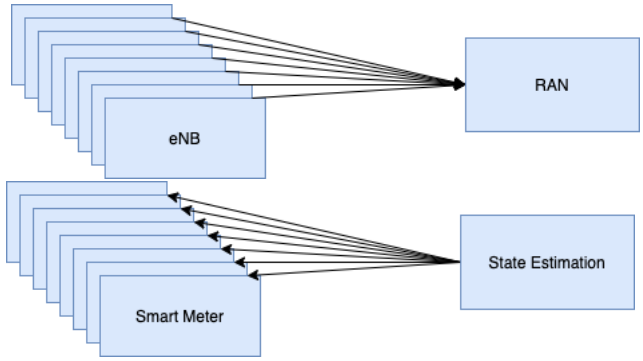

Figure A.5: In these two situations, the number of agents is two high to manually initialise and a automatic cloning is initiated. It is important for the simulation to represent the situations where a number of base stations (eNB) will have a OL of 0 if the RAN fails, but will not have experienced a an failure which can be repaired internally. In the bottom case the Sate Estimation in the smart grid will have a OL of 0 if a number (higher than R) of smart meters fail, or get reduced OL.

A.3 Model Implementation

A.3.1 Agent Initialisation

In modelling some of the entities a multiple to one agent is needed, for example eNBs in the 5G transportation network, where the RNC is dependant on a high amount of eNBs.

A.3.2 Initialisation of the Simulator

The "Infrastructure Model"-class is the initialisation class and essentially builds the model using the "EntityAgent" class. In this class every agent is initialised with the appropriate parameters, and the JADE agent management system is lunched.

A special class for initialisation of multiple to one agents, as seen in Figure A.5 was also developed to ease the practicality of initialisation many agents with the same dependencies, like the PMUs and RTUs. In Figure A.6, the model is initialised, and the PMUs and RTUs are put in separate containers. The different containers (icons as green folders) have no function for the simulation dynamics, and are only organisational support. The "Main-container" contains different support-agents automatically initialised by the JADE tool.

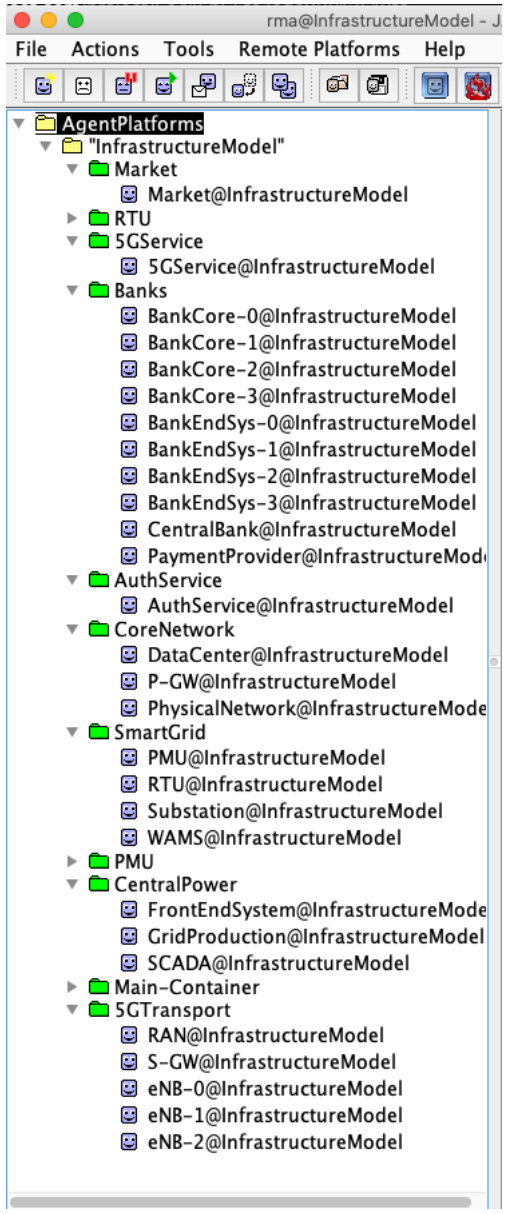

Figure A.6: Screenshot of the JADE-tools gui, with all containers and agents initialised. The containers serve no function other than the organisational. The 30 PMUs and 10 RTUs agents are kept in containers for easy overview. The agents just called "PMU" and "RTU" are created for the container initialisation and does not interact directly with the simulation.

A.3.3 *Entity Agent* Class

The primary class developed to describe the behaviour of infrastructure components. Note that there is some adjustments to fit the written format of the thesis.

```
package simpleEntity;

import java.io.IOException;
import java.util.Arrays;
import java.util.Random;
import java.util.logging.FileHandler;
import java.util.logging.Level;
import java.util.logging.Logger;
import java.util.logging.SimpleFormatter;
import java.util.HashMap;
import java.util.Map.Entry;

import jade.core.AID;
import jade.core.Agent;
import jade.core.behaviours.Behaviour;
import jade.core.behaviours.CyclicBehaviour;
import jade.core.behaviours.TickerBehaviour;
import jade.lang.acl.ACLMessage;
import jade.lang.acl.UnreadableException;
import jade.util.leap.Iterator;
import jade.wrapper.AgentController;

public class EntityAgent extends Agent{

  private Double failureRate = 0.0;

  private double OL = 1.0;
  private boolean F = false;
  private double R;
  private int restorationTime;
  private double totalOL;

  static Logger logger = Logger.getLogger("global");

  private HashMap<AID, Double> OutConnectedAgents =
                        new HashMap<AID, Double>();
  private HashMap<AID, Double> InConnectedAgents =
```

```
                    new HashMap<AID, Double>();

Object[] args;



protected void init() {

      // Printout a welcome message
      Iterator it = getAID().getAllAddresses();
      while (it.hasNext()) {
              System.out.println("- "+it.next());
              }

      args = getArguments();

      System.out.println("Agent "+ getAID().getLocalName() +
      "("+ getAID().getName() + ") is running with init values:");
      if (args != null) {
              for (int i = 0; i < args.length; ++i) {
                      System.out.println("- "+ args[i]);
              }
      }

      setfailureRate( Double.parseDouble( (String) args[0]));
      initQuantities(Double.parseDouble( (String) args[1]),
                     Integer.parseInt( (String)args[2]) );

      addBehaviour(reciever);
      addBehaviour(restoreCheck);
      addBehaviour(failureCheck);


      try {
              Thread.sleep(3000);
      } catch (InterruptedException e) {
              e.printStackTrace();
              }

      sendOL();
```

```
  }

  protected void initQuantities(double Requirements, int RestorationTime){

        setR(Requirements);
        setRestorationTime(RestorationTime);

        for(int i = 3; i < args.length; ++i) {
          if(getOutConnectedAgents()
                .containsKey(new AID((String) args[i],
                                AID.ISLOCALNAME))){
                continue;
          }

          getOutConnectedAgents()
                .put(new AID((String) args[i], AID.ISLOCALNAME), 1.0);
          System.out.println("Adding OutAgent: " +
                          new AID((String) args[i],
                              AID.ISLOCALNAME).getLocalName());

        }

        sendOL();
};


/**
* Agent clean-up */
protected void takeDown() {
// Printout a dismissal message
        logger.info( getLocalName() + ";"+
                     getOL() + ";" +
                     getInConnectedAgents() + ";" +
                     getOutConnectedAgents() + ";");
        System.out.println(getAID().getLocalName()+" is terminating.");
}


private Double getfailureRate() {
        return failureRate;
}
```

```
public void setfailureRate(Double failureRate) {
        this.failureRate = failureRate;
}


public double getOL() {
        return OL;
}

public void setOL(double oL) {

        if(oL != OL) {
                OL = oL;
                sendOL();
                logger.info( getLocalName() + ";"+
                             getOL() + ";" +
                             getInConnectedAgents() + ";" +
                             getOutConnectedAgents() + ";");

        }


}


public boolean isF() {
        return F;
}

public void setF(boolean f) {
        F = f;
}


public double getR() {
        return R;
}

public void setR(double r) {
        R = r;
}
```

```
private void sendOL() {

  for (Entry<AID, Double> Agent : getOutConnectedAgents().entrySet()) {
        ACLMessage msg = new ACLMessage(ACLMessage.INFORM);
        try {
                msg.setContentObject( getOL() );
        } catch (IOException e) {
                e.printStackTrace();
        }
        msg.addReceiver( Agent.getKey());
        send(msg);
  }

        try {
                Thread.sleep(1000);
        } catch (InterruptedException e) {
                e.printStackTrace();
                }
};
```

```
CyclicBehaviour reciever = new CyclicBehaviour(this) {
  public void action() {
        ACLMessage msg = myAgent.receive();

        if(msg != null) {
          if(!getInConnectedAgents().containsKey(msg.getSender())) {
                getInConnectedAgents().put(msg.getSender(), 1.0);
          }

          if( ACLMessage.getPerformative(
                msg.getPerformative()) == "INFORM"){

            try {
                    getInConnectedAgents().replace(
                                        msg.getSender(),
                                (double) msg.getContentObject()
```

```
                                        );
                } catch (UnreadableException e) {
                        e.printStackTrace();
                }
              }
            }
        }
```

```
TickerBehaviour restoreCheck = new TickerBehaviour(this, 10) {

  public void onTick() {
        //checks if the Operational Level satisfies the Requirements
        double totalDependencies = getInConnectedAgents().size();
        totalOL = getInConnectedAgents().values().stream()
                  .mapToDouble(Double::doubleValue).sum();

        if(getInConnectedAgents().size() < 1) {
                totalOL = 1;
        }

        if(totalDependencies < 1) {
                totalDependencies = 1;
        }


        setOL( totalOL / totalDependencies);

        if(getOL() < getR()){
                setOL(0.0);
                System.out.println(getAID().getLocalName() +
                ": Suffered a failure due to low Operation Level.");


        }

        if(isF()){
                restoration();
        }
  }
```

```
};

TickerBehaviour failureCheck = new TickerBehaviour(this, 10) {
        @Override
  protected void onTick() {
        // Rolls random if the agent should fail or not
        if(new Random().nextDouble() <= getfailureRate()){
          setOL(0.0);
          setF(true);

        System.out.println(getAID().getLocalName() +
                ": Suffered an INTERNAL failure.");
        }
  }
};
// Emergency logger
TickerBehaviour logging = new TickerBehaviour(this, 10000) {
  @Override
  protected void onTick() {
        logger.info( getLocalName() + ";"+
                     getOL() + ";" +
                     getInConnectedAgents() + ";" +
                     getOutConnectedAgents() + ";");
  }
};

private void restoration() {

        try {
                Thread.sleep(getRestorationTime());
        } catch (InterruptedException e) {
                e.printStackTrace();
        }
        setOL(1.0);
        setF(false);
        System.out.println(getAID().getLocalName() + " Restored");

}


public int getRestorationTime() {
```

```
        return restorationTime;
}

public void setRestorationTime(int restorationTime) {
        this.restorationTime = restorationTime;
}

public HashMap<AID, Double> getInConnectedAgents() {
        return InConnectedAgents;
}

public void setInConnectedAgents(
            HashMap<AID,Double> inConnectedAgents) {
        InConnectedAgents = inConnectedAgents;
}

public HashMap<AID, Double> getOutConnectedAgents() {
        return OutConnectedAgents;
}

public void setOutConnectedAgents(
            HashMap<AID, Double> outConnectedAgents) {
        OutConnectedAgents = outConnectedAgents;
}

}
```

A.3.4 Model Initiation Example

All agents are initialised in one class called *infrastructure model*. Below is an example of how the 5G service agent is initialised.

```
private void start5GService() {
        Runtime rt = Runtime.instance();
        // Create a default profile
        Profile p = new ProfileImpl();
                    p.setParameter(
                                    Profile.CONTAINER_NAME,
                                   "5GService");

        // Create a new non-main container, connecting to the default
```

```
        // main container (i.e. on this host, port 1099)
        ContainerController cc = rt.createAgentContainer(p);

        AgentController agent;

        //CoreNetwork

        Object GSArgs[] = new Object[10];
        GSArgs[0] = lowFailureRate; //FailureRate
        GSArgs[1] = "0.7";//Requirements
        GSArgs[2] = restorationTime;//RestoreTime

         //Sendring OL to agents:
        GSArgs[3] = "WAMS";
        GSArgs[4] = "BankEndSys-0";
        GSArgs[5] = "BankEndSys-1";
        GSArgs[6] = "BankEndSys-2";
        GSArgs[7] = "AuthService";
        GSArgs[8] = "PaymentProvider";
        GSArgs[9] = "Market";

        try {
          agent = cc.createNewAgent("5GService" ,
                                    "simpleEntity.SimpleEntity",
                                    GSArgs);
          agent.start();
        } catch (StaleProxyException e) {
          e.printStackTrace();
        }
}
```

A.3.5 Data Processing With Pandas and Plotly

The simulation results are processed using a Python based script with Pandas and Plotly packages.

```
import pandas as pd
import csv
import os
import xml.etree.ElementTree as et
import numpy as np
```

```
import matplotlib.pyplot as plt
from matplotlib.collections import PolyCollection
from mpl_toolkits.mplot3d import axes3d, Axes3D
from matplotlib.widgets import Slider



#plt.close('all')
#plt.style.use('ggplot')

def parse_XML(xml_file, df_cols):
    """Parse the input XML file and store the result in a pandas
    DataFrame with the given columns.

    The first element of df_cols is supposed to be the identifier
    variable, which is an attribute of each node element in the
    XML data; other features will be parsed from the text content
    of each sub-element.
    """

    xtree = et.parse(xml_file)
    xroot = xtree.getroot()
    rows = []

    for node in xroot:
        res = []
        res.append(node.attrib.get(df_cols[0]))
        for el in df_cols[1:]:
            if node is not None and node.find(el) is not None:
                res.append(node.find(el).text)
            else:
                res.append(None)
        rows.append({df_cols[i]: res[i]
                     for i, _ in enumerate(df_cols)})

    out_df = pd.DataFrame(rows, columns=df_cols)

    return out_df


col_names = ["date","millis",
```

```
            "sequence","logger",
            "level","class",
            "method","thread",
            "message"]
df = parse_XML("simResults.xml", col_names)

df = df.join(df["message"].
            str.split(';', expand = True)
            .rename( columns = {0:"agent",
                                1:"OL",
                                2:"InAgents",
                                3:"Outagents"}))

df["OL"] =  pd.to_numeric(df["OL"],errors = "coerce")
df = df.replace(np.nan, 0, regex = True)

df_ol = df[["millis","agent","OL"]]
df_grouped = df_ol.groupby("agent")
df_grouped = df_plot.filter(lambda g: (g.OL == 0.0).all())

#Enter entities for creating subplots:
selected_entities = ["eNB-0","eNB-1","WAMS","PaymentProvider","5GService"]

df_pivot = df_ol.pivot_table(index = 'millis', columns='agent', values ='OL')

#For filtering out the PMU and RTU traces
df_pivot = df_pivot[df_pivot.columns.drop(list(df_pivot.filter
                                        (regex='PMU*')))]
df_pivot = df_pivot[df_pivot.columns.drop(list(df_pivot.filter
                                        (regex='RTU*')))]
df_pivot = df_pivot[df_pivot.columns.drop(list(df_pivot.filter
                                        (regex='eNB*')))]
selected_entities = df_pivot.columns
df_pivot = df_pivot[selected_entities]

df_pivot = df_pivot.fillna(method='ffill')
df_pivot = df_pivot.fillna(1.0)
```

Plotting Component OL Trace

```
plt.close('all')
print(df_pivot)
```

```
fig, axes = plt.subplots(nrows=len(df_pivot.columns))

for i in range(0,len(axes)):
    df_pivot[selected_entities[i]].plot(ax = axes[i], subplots=True, legend = Fals
    axes[i].set_ylim([0.0, 1.0])
    axes[i].set_ylabel(df_pivot.columns[i])

plt.suptitle('Agent operational levels')
plt.xlabel('Time')
plt.tight_layout()
plt.show()
```

Analysing Steady-State Simulation

```
Timespan = (int(df_pivot.index[-1]) - int(df_pivot.index[0]))
print("Simulation timespan: " + str(Timespan) + " millis \n")
print("Days: " + str(Timespan/10))
print("Years: " + str((Timespan/10)/365))

df_failures = pd.DataFrame()
df_failures['meanOL'] = df_pivot.mean()

df_varStd = pd.DataFrame()
df_varStd['std'] = df_pivot.std()

for agent in df_pivot.columns:
    print(df_pivot[agent].describe())

print("NUMBER OF FAILURES:\n")
print(df_failures.to_string())

ax= df_failures.plot.bar(label='meanOL')
ax= df_varStd.plot.bar(label='std')

plt.show()
```

A.4 Model Design

Final sheet of components gathered from the systematic literature review is attached on the next pages. Some components were left out of the final model and is therefore strikethroughed.

Financial				
System	Component	Description	Dependencies	Failure Rate
Market	Market	Facilitates energy pricing	Front end service(power), Banking, payment providers	Medium
Central Bank	RTGS	Central component of the Central bank, completes all national settlements	Physical Network	Low
Auth service	Authentication	Authenticates bank customers	5GService	Medium
Commercial banks	Core banking system	Processes customer interactions and transactions inside each commercial bank	RTGS	Low
	End user systems	Customer interactions, mobile banks, etc.	5G Services, Core banking systems, Authentication systems	High
Payment providers	Payment processors	Third party payment processors	Central Bank, Core Banking systems, EndPower systems	Medium
Communications				
System	Component	Description	Dependencies	Failure rate
Core Network (CN)	~~Operations and management~~	~~Simplifying operations and management. Routing and providing services to the network. Consisting of SDN controllers, and Routers.~~		
	Physical network	The connections between endpoints and central processing. In the 5G it will be a minimized number of entities and functionalities.		Low
	Data centers (DC)	To run computations to support MEC service data centers are necessary. These data centers are deployed in close vicinity to the eNB's on a large-scale for MEC service, and more centralized in the MCC service.		Low
	Packet Data Network Gateway (P-GW)	The gateway between P-GW and external networks (internet), Policy and Charging Rules (PCC), MCC (Data centers)	Physical Network, DC	Low
5G (RAN)	NG-Radio Access Network (RAN)	Connects a set of eNBs, with the core RNC	S-GW	Low
	eNB	Base stations, and end-users entrypoint	RAN	Medium
	Serving Gateway (S-GW)	Gateways from the base stations (eNB) to the P-GW	P-GW	Medium
5G services	mobile edge computing (MEC)	will be key for the deployment of the aforementioned distributed SE approaches. Distributed SE can be integrated into the framework of MEC, while acquiring measurements via 5G MTC services. Multi-Access Edge Computing (MEC) is an important element of 5G architecture. MEC is an evolution in cloud computing that brings the applications from centralized data centers to the network edge, and therefore closer to the end users and their devices. This essentially creates a shortcut in content delivery between the user and host, and the long network path that once separated them.		
	ultra-reliable low-latency communications (URLLC) services	Required for the WAMS	DataCenters	

	Network function Virtualization (NFV)	decouples software from hardware by replacing various network functions such as firewalls, load balancers and routers with virtualized instances running as software. This eliminates the need to invest in many expensive hardware elements and can also accelerate installation times, thereby providing revenue generating services to the customer faster.		
	Mission Critical Communications (MCC)	is one of the key elements of the new 5G build out. Started with 3GPP Release 13, Mission Critical Communications are delivered as the core network service allowing First Responders – police, firefighters and emergency medical personnel – to replace outdated radio with modern communication capabilities which are readily available to any smartphone user today.		Low
Power systems				
System	Component	Description	Dependencies	Failure Rate
Central power system	Front end service	The power companies communication channel with customers. The way customers can check predicted power usage, and production.	SCADA, 5GService	High
	SCADA	services of supervision, control and data acquisition (SCADA) system, which constitutes the nervous system of a power grid. In turn, SCADA services depend on the availability of the interconnected networks supporting such services.	Physical Network	Low
	~~Recovery SCADA~~	~~Unmanned SCADA control center~~		
	~~Aggregated data processing~~	~~Systems for aggregating system data, for processing and analysis.~~		
	~~Central Production and Grid~~	~~Bulk movement of electrical energy from a generating site, such as a power plant, to an electrical substation.~~		
Smart Grid	Substation	Transformers from high to low voltage. Automated stations in the Smart Grid	SCADA	Low
	Phasor measurement units (PMUs)	Accurately measure voltage and current phasors at high sampling rates. Exploiting PMU inputs for a robust, decentralized, and real-time SE solution calls for novel communication infrastructure that would support the future wide area monitoring system (WAMS).	WAMS, eNB	Medium
	Future wide area monitoring system (WAMS)	WAMS aims to detect and counteract power grid disturbances in real time.	PMU, RTU, 5GService	Low
	Remote Terminal Units (RTU)	Part of the SCADA systems. interface the SCADA with the power distribution grid at high voltage (HV) (Pi boxes) and medium voltage (MV) (Mi boxes) substations.	eNB, Substation	Medium
	~~Default proprietary network (DPN)~~	~~serially connects the SCADA control centres to HV RTUs.~~	~~SCADA, RTUs~~	
	~~Smart Meters~~		~~eNB~~	