NTNU – Trondheim
Norwegian University of
Science and Technology

Dependability in Interdependent Digital Ecosystems

Martin Hagen Hettervik

Master of Science in Communication Technology
Submission date: June 2015
Supervisor: Poul Einar Heegaard, ITEM

Norwegian University of Science and Technology
Department of Telematics

Title: Dependability in Interdependent Digital Ecosystems

Student: Martin Hagen Hettervik

Problem description:

The integration of information and communications technology (ICT) into common systems like power grids, and the interconnection of ICT and power grid systems, creates digital ecosystems. Such systems have increased dependencies compared to traditional power grids, like reliance on information for monitoring and controlling. The modeling of digital ecosystems may not be a trivial matter because of complexity and state space explosion. For the system modeling and dependability analysis it is critical to have an overview of what types of dependencies that exist in the system, what components they affect, and how the dependencies influence the system as a whole.

As digital ecosystems play critical roles in our society, the prediction of their dependability is of importance and in need for further research to ensure that the services they deliver are safe and reliable. The objective behind this thesis is to investigate the types of dependencies that could realistically exist in digital ecosystems and how to model those dependencies in order to analyse the system dependability.

A single digital ecosystem will be used for all modeling to ensure a common foundation when analysing the effects of different types of dependencies in the system. The digital ecosystem that will be used is a smart grid system, a power grid improved by information and communications technology.

The first part of this thesis will investigate what types of dependencies that could realistically exist in a smart grid, and thus the extent to which interdependencies could manifest in such a system. Based on the findings of the first part, the second part of this thesis will investigate how to model and analyze the dependability of a smart grid with different types of dependencies. With the investigation of smart grid interdependencies and modeling shown, a discussion of the takes on the system modeling will be presented, along with a final conclusion proposing what modeling takes to use when different types of dependencies are existent in a digital ecosystem.

Responsible professor: Poul E. Heegaard, ITEM

Supervisor: Jonas Wäfler, ITEM

Abstract

Advances in information and communications technology (ICT) encourages the interconnection of ICT systems with traditional monolithic systems, creating complex systems of systems. A modern variety of such systems is the digital ecosystems, including smart grids, which are introduced to new types of dependencies and failures not previously applicable, particularly the introduction of interdependencies between systems. Because of this, new approaches for dependability analysis are needed to further ensure safe and reliable services.

In the first part of this thesis the presumably most relevant interdependencies and failures in smart grids are identified through a study of literature, categorized along the dimensions of *type of interdependency* and *type of failure*, and found to be; (1) cascading failures in physical interdependencies, (2) escalating failures in cyber interdependencies, and (3) common cause failures in geographic interdependencies.

The second part of this thesis shows dependability modeling approach proposals for the identified relevant combinations of interdependencies and failures. Numerical results from the dependability models reveals that some conceivable smart grid failures have bigger effects than others; (1) cascading failures in power grids and (2) common cause base station (BS) failures due to natural events like storms or human caused events like BS disrupting construction work. In addition, it is shown that malware in smart grids can exist and propagate without detection and should be a legitimate concern of stakeholders.

Sammendrag

Fremskritt innenfor informasjons- og kommunikasjonsteknologi (IKT) har oppmuntret til sammenkobling av IKT systemer og tradisjonelle monolittiske systemer, noe som skaper komplekse systemer av systemer. En moderne variant av slike systemer er digitale økosystemer, inkludert smarte nett, som er introduserte til nye typer av avhengigheter og feil ikke tidligere aktuelle, spesielt innføringen av gjensidige avhengigheter mellom systemer. På grunn av dette er nye tilnærminger til pålitelighetsanalyse nødvendig for å ytterligere forsikre trygge og pålitelige tjenester.

I den første delen av denne avhandlingen er de antatt mest relevante gjensidige avhengigheter og feil i smarte nett identifisert igjennom en litteraturstudie, kategorisert langs dimensjonene *type gjensidig avhengighet* og *type feil*, og funnet til å være; (1) kaskaderende feil i gjensidige fysiske avhengigheter, (2) eskalerende feil i gjensidige cyberavhengigheter, og (3) feil med felles årsak i gjensidige geografiske avhengigheter.

Den andre delen av denne avhandlingen viser forslag til tilnærminger for pålitelighetsmodellering for de identifiserte relevante kombinasjonene av gjensidige avhengigheter og feil. De numeriske resultatene fra pålitelighetsmodellene viser at noen typer feil i smarte nett har større effekter enn andre; (1) kaskaderende feil i kraftnett og (2) basestasjonsfeil med felles årsak som følge av naturlige hendelser som stormer eller menneskeskapte hendelser som basestasjonsforstyrrende anleggsarbeid. I tillegg er det vist at skadeprogrammer i smarte nett kan eksistere og propagere uten å bli oppdaget, og bør derfor være en legitim bekymring for interessenter.

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Traditional dependability analysis of systems has relied on the simplifying assumption that the systems being analysed are monolithic. With advances in information and communications technology (ICT), systems providing new abilities and functions have been interconnected with the previously assumed monolithic systems, creating advanced collaborations of systems working together for a common goal. A collaboration of systems like this is called a *system of systems*, and is in many ways qualitatively different from traditional large-scale systems [Fis06].

A system of systems that is distributed, adaptive, and open socio-technical is sometimes referred to as a *digital ecosystem*. Such systems are characterized by self-organization, autonomous subsystems, continuous evolution, scalability and sustainability, providing both economic and social value [BC07]. An example of a modern digital ecosystem is the *smart grid*, a power grid using ICT for monitoring and managing of power transport and generation. Technologies in smart grids helps consumers balance supply and demand, optimise the use of power grid assets, and provides resiliency to disturbances, attacks and natural disasters [Int11].

It is clear that smart grids and other digital ecosystems have advantages compared to traditional large-scale monolithic systems. However, with increasing ICT dependencies, numerous subsystems and components, and lack of coordinated management, the prediction and assess of the digital ecosystems' dependability may not be of a trivial matter. Many of the approaches of traditional systems' dependability analysis are ineffective and sometimes counterproductive for modern digital ecosystems, therefore new ways for dependability analyses are needed in these sort of systems.

Because of the critical roles digital ecosystems like smart grids play in our society the prediction of these systems' dependability is of importance and in need for further research to ensure safe and reliable services. This thesis should give the reader insight in and awareness of how dependencies and failures behave in and affect digital ecosystems, especially dealing with smart grids. The findings and suggestions from

this thesis are intended as a guideline for dependability analyses in today's and future digital ecosystems, both with regard to what types of dependencies and failures stakeholders should lay focus on and what approaches for dependability modeling to use.

1.1 Outline

Part I in this thesis first classify types of dependencies and failures that are deemed relevant for digital ecosystems. With the classifications covered, an investigation of possible dependencies and failures in smart grids is performed to get a better understanding of how dependencies can manifest and failures propagate in digital ecosystems like smart grids. The investigation will identify the presumably most relevant types of dependencies and failures in smart grids and in this way set a focus for further dependability analyses.

In Part II a smart grid system is first defined to ensure a common basis for all ensuing dependability modeling and analyses. With the smart grid system defined, six use cases are presented covering all presumed relevant types of dependencies and failures from the investigation in Part I. The use cases are modeled and analysed one by one, giving both insight in approaches for dependability modeling in smart grids and the effects of dependencies and failures shown by the numerical results obtained.

With the relevant smart grid dependencies and failures analysed, a discussion of the dependability modeling approaches made and the numerical results from the use cases is done. Lastly, a final conclusion is presented, proposing what dependability modeling approaches to use when different types of dependencies and failures are present in a digital ecosystem. The conclusion will also suggest some possible future work for this field of study.

1.2 Related Work

To get an overview of dependencies in infrastructures, [RPK01] presents a conceptual high level framework. More relevant to power grids and ICT, [LKK07] provide models characterizing interdependency related failures in power systems and associated ICT systems. Further on, [KB09] proposes a framework for analysing the impact that ICT failures can have on power systems and identifies some of the challenges posed by the increasing reliance on ICT. For smart grids in specific, [WH13b] study dependencies in and the influence ICT may have on dependability, and [WH13a] show an approach for dependability analysis combining structural and dynamic models.

Part I

Principles of Interdependencies

Chapter 2
Classifications of System Dependencies and Failures

This chapter presents definitions and classifications of dependencies and failures, and explains the theory and concepts behind how failures can propagate in systems of systems. The classifications and concepts gone through in this chapter build the foundation for the following investigation, analyses, and discussion.

2.1 Dependencies and Interdependencies

A dependency is *"a linkage or connection between two systems, through which the state of one system influences or is correlated to the state of the other"* [RPK01]. For example, a power grid system could be dependent on a control system for management of power production and transmission, and a ICT network system could be dependent on a power grid for the continuous supply of power, illustrated in Figure 2.1. In a case like this, if the power grid fails, the ICT network is no longer supplied with power and thus fails as well. Also, if the control system fails, the power grid would lose crucial management and fail, and hence the ICT network would fail too. In this example the power grid is dependent on the control system and the ICT network is dependent on the power grid, implying that the ICT network is dependent on the control system as well.

An interdependency is *"a bidirectional relationship between two systems through which the state of each system influences or is correlated to the state of the other. More generally, two systems are interdependent when each is dependent on the other"* [RPK01]. However, the relationships between systems that create interdependencies are not necessarily direct and intuitive, but could rather be characterized by multiple dependencies among systems. Assume, as in the example before, that a control system is needed for managing a power grid, and power from a power grid is required for sustaining a ICT network. In addition, assume that a ICT network is needed for delivering information and commands to and from the control system, which could be the same as the one mentioned ICT network dependent on the power grid.

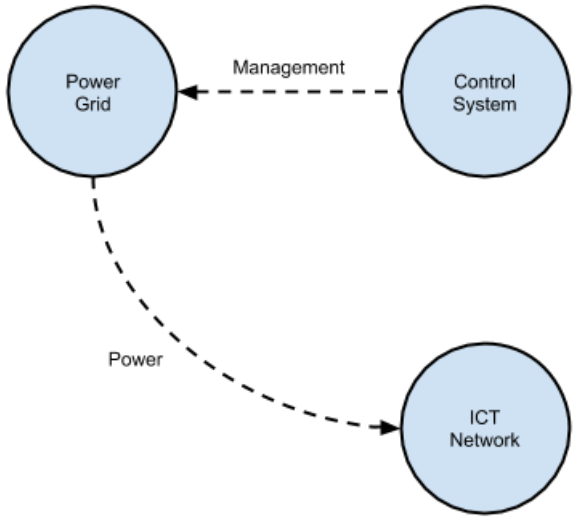

Figure 2.1: Example of system dependencies in a system of systems.

This example is illustrated in Figure 2.2 and shows how system dependencies can create interdependencies within a system of systems. In the presented example, the ICT network depends on power from the power grid, and the power grid is likewise dependent on the ICT network for delivering information and commands to and from the control system, meaning they are interdependent. Implicitly, when more systems and dependencies are added into a system of systems the complexity grows.

Interdependencies are often between only two systems. From the previous examples one can imagine that the control system, as well as the ICT network, depends on power from the power grid. In that case an ever simpler interdependency is perceived, made out of only two system dependencies, the power grid depending on management from the control system, and the control system depending on power from the power grid. This simple form of interdependency is demonstrated and analysed in greater detail in Part II of this thesis.

2.2 Dimensions of Interdependencies

[RPK01] has described six dimensions of interdependencies intended to facilitate the identification, understanding and analysis of interdependencies; *type of failure*, *system characteristics*, *state of operation*, *type of interdependency*, *environment*, and *coupling and response behavior*.

The objective behind this thesis is to investigate what types of dependencies that could realistically exist in digital ecosystems and look at how to model these

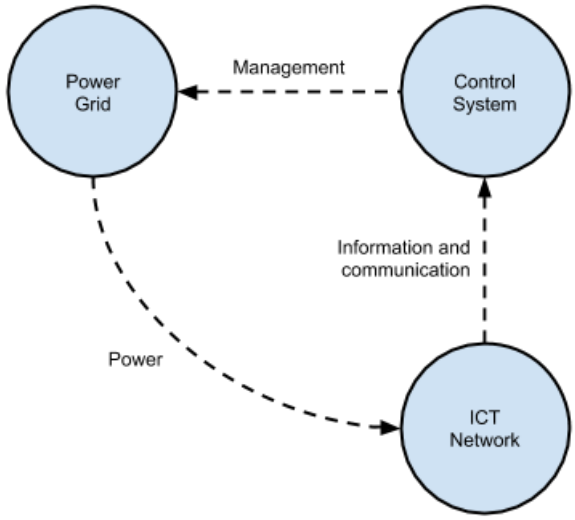

Figure 2.2: Example of system dependencies creating system interdependencies in a system of systems.

dependencies in order to analyse the system dependability. For this objective two of the dimensions of interdependencies are particularly interesting, namely *type of failure* and *type of interdependency*, which describe the nature of a interdependency and how a failure behave as a consequence of interdependencies. Because of this, these two dimensions are explicitly studied in in the following investigation of dependencies and failures.

2.2.1 Types of Interdependencies

Besides the topology of how systems are dependent on each other with directional or bidirectional relationships, dependencies can exist in several ways between systems. [RPK01] has defined four principal types of interdependencies, each with its own characteristics and effects on systems.

Physical interdependency

"Two systems are physically interdependent if the state of each is dependent on the material output(s) of the other."

Cyber interdependency

"A system has a cyber dependency if its state depends on information or commands transmitted through some ICT system."

Geographic interdependency

"Systems are geographically interdependent if a local environmental event can create state changes in all of them."

Logical interdependency

"Two systems are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection."

Going back to the example from Figure 2.2, the existing dependencies in the system of systems can be classified. The power grid has a cyber dependency to the control system as it depends on management in form of digital commands over a ICT network, and the said ICT network has a physical dependency to the power grid as it depends on the power grids physical output, power. For the control system to send commands to the power grid, a physical ICT network of cables and switches is needed, and therefore the dependency from the control system to the ICT network could be regarded as a physical dependency. Additionally, for the control system to make decisions on a sound basis it would need digital information from the power grid delivered over the ICT network, meaning that the dependency to the ICT network could also be a cyber dependency. This shows that although the described types of dependencies have distinct characteristics, they are not necessarily mutually exclusive, but for the sake of simplicity a dependency can often be distinctly classified based on its dominating attributes.

2.2.2 Types of Failures

Interdependencies between systems increase the risk of errors and failures in a system of systems. Complex topologies created by interdependencies can initiate and propagate disturbances in a variety of ways that are unusual and difficult to foresee. To systematize the ways in which errors and failures in systems can propagate and disrupt the states of other systems this thesis uses the three classified types of failures proposed by [RPK01].

Cascading failure

"A cascading failure occurs when a disruption in one system causes the failure of a component in a second system, which subsequently causes a disruption in the second system."

Escalating failure

"An escalating failure occurs when an existing disruption in one system exacerbates an independent disruption of a second system, generally in the form

of increasing the severity or the time for recovery or restoration of the second failure."

Common cause failure

"A common cause failure occurs when two or more systems are disrupted at the same time; components within each system fail because of some common cause. Components from multiple systems could be affected simultaneously, either because the components occupy the same physical space or because the root problem is widespread."

For the previous example from Figure 2.2 this means, if the ICT network loses power due to an internal failure in the power grid, the power grid failure has cascaded to the ICT network. If the power grid and ICT network where to be located in the same geographically area they would also have a geographic interdependency. In this case an environmental event, e.g. construction work, could disrupt both systems simultaneously creating a common cause failure. The cyber dependency from the power grid to the control system could conceivably give rise to both cascading and escalating failures. If the power grid would fail without management provided by the control system, a failure in the control system would be of a cascading type. Alternatively, if the power grid keeps on working even if the control system fails, an internal failure in the power grid may get more severe consequences than if the control system had worked when the failure occurred, e.g. in the form of increased time for failure detection and location. In this case the control system failure would be an escalating failure.

From the definition of cascading failures and the previous examples it is understood that if a failure in a system is to cascade, it has to cause a disruption in another system. Consequently, a failure in a component causing a failure of a second component in the same system is not per definition a cascading failure. In this thesis, to differentiate between cascading failures and failures contained within a single system, the latter is referred to as a *propagating failure*.

Chapter 3
Dependencies and Failures in Smart Grid Systems

In this chapter a literature review is conducted to investigate possible interdependencies and failures in systems of systems, specifically digital ecosystems. The considered digital ecosystem is the future power grid, also known as smart grid. Already the traditional power grid is dependent on ICT networks and control systems, as shown in the examples in Chapter 2. The smart grid is going to include even more ICT devices and services, making it on one hand smarter, but on the other hand adding dependencies and complexity [Int11] [KB09].

Studies on ICT networks and power grid systems have indeed shown that failures in these systems are not independent but rather correlated. To clarify what types of interdependencies that will most realistically exist in and what types of failures that will occur in smart grid system of systems, scenarios and examples recognized from study of literature are presented in the following sections. The presented scenarios and examples are sorted by the classified failure types from Section 2.2.2, where for each failure type all relevant types of interdependencies from Section 2.2.1 are examined, revealing how failures can affect smart grids in different ways. The logical interdependency type is not analysed further as it is presumed to be of little relevance for the types of failures that can occur in smart grids.

3.1 Cascading Failure

As smart grids highly rely on interdependent power grid, telecommunication and ICT systems there are several ways in which failures can cascade between components and systems within smart grid systems. Components in telecommunication and ICT systems could be dependent on power from power grids, stress and congestion may spread between networks, or malware in software (SW) could cascade between ICT components in different systems [BPP+10] [WH13b].

3.1.1 Physical Interdependency

In power grid, telecommunication and ICT systems disturbances can propagate quickly through the networks. Increased stress caused by natural disasters, purposeful attack, or unusually high demands can cause components in the systems to fail, leading to increased stress on remaining components and eventually the failure of whole systems. In the same way stress propagate between components, failed systems may cascade stress to other systems [Ami00].

A cascading failure over physical interdependencies occurred in Italy on 28 September 2003, starting with a transmission line shutting down following a flashover between a conductor cable and a tree. Because the power grid operators did not manage to reorganize production and export capacities in time, a series of failures in other transmission lines followed, giving rise to a blackout throughout Italy. The failure of power grid components directly led to failures of dependent ICT network components, which in turn caused further failures in power components [BN03] [BPP+10].

On 8 September 2011 a power grid system disturbance happened in the Pacific Southwest leading to cascading failures and leaving approximately 2.7 million customers without power. The loss of a single high power transmission line started the event, causing power flows to be instantaneously redistributed throughout the power grid. Sizable voltage deviations and component overloads were caused due to the redistribution, creating a ripple effect of components failing [ASC12].

3.1.2 Cyber Interdependency

An error in an ICT component may cascade errors to other ICT components by spreading harmful configuration or malware, which could linger in components undetected. Unless treated, ICT errors will accumulate in ICT systems and eventually lead to failure [LKK07]. As power grid control systems relies on interconnecting ICT systems, failures in ICT systems can lead power grid systems to a vulnerable state. Frequency of failures cascading due to malicious intention in ICT systems has been on the rise, including among others worm and virus attacks, and is today a legit concern of stakeholders [RBM09].

3.1.3 Geographic Interdependency

If two or more components from different systems share a common geographic location a failure could cascade from one system to another even though the systems do not share resources or services besides location, e.g. if one of the systems cause a fire or explosion [SOK+13]. If a BS belonging to a telecommunication system stands next to a power grid transmission line, a voltage overload in the power grid could cause

components in the transmission line to overheat and catch fire, in which case the fire could spread to the BS.

3.2 Escalating Failure

In smart grid systems escalating failures could be failures in monitoring systems that restrain detection of failures in power grids, failures in control systems causing them to misbehave when dealing with other disruptions, or failures that prevent actions being taken against critical situations. These are all examples of escalating failures that not necessarily cause significant trouble to operators or customers alone, but can cause a potential subsequent failure to have a worse impact than if it had happened without the simultaneous escalating failure [LKK07] [KB09]. These systems monitoring and controlling power grids are regularly in the ICT and SW domain, therefore only cyber interdependencies are relevant when studying escalating failures in smart grids.

An ICT system failure causing failure escalation happened in the U.S. and Canada on 14 August 2003. Inaccurate input data rendered a system monitoring tool ineffective concurrently as some power grid transmission lines failed when tripping due to overgrown trees. The ineffective monitoring tool prevented confining the transmission line incidents, causing heavy loading on parallel circuits, leading to a trip of a key transmission line. The failure of the key transmission line triggered a cascade of interruptions on the high voltage power grid system [PSO04].

3.3 Common Cause Failure

Common cause failures in smart grids can happen either because smart grid components occupy the same physical space, components rely on a common fallible service, or the root problem is widespread, e.g. if maintenance errors, distribution of faulty software updates or erroneous configuration affect many components at the same time [WH13b].

3.3.1 Physical Interdependency

If an operator is leasing from the system of another operator, e.g. if a mobile network operator (MNO) is leasing capacity from the network of another MNO, a failure in the system would affect both the owning and leasing operator [FH11]. Similarly, if several systems rely on the output of a common physical system, as seen regularly with power grids supporting everyday infrastructure, a failure in the physical system would affect all dependent systems.

An example of a common cause failure happened on 4 November 2006 in Northern Germany. The disconnection of a high-voltage transmission line split the Western European power grid into three separate areas with significant power imbalances in each area. The power imbalance in the westernmost of the areas induced a severe frequency drop that caused an interruption of power supply for more than 15 million European households [FRS07].

3.3.2 Cyber Interdependency

If a failure happens in an ICT system it may lead to a common failure in other systems relying on the services of the failed system, e.g. in the form of deficient information, monitoring or communication. Concerning malware and cyber attacks, in smart grids with integrated ICT systems, a failure in an ICT component could instantaneously spread to several other ICT components if they share configuration or SW implementation. Especially regarding cyber attacks there is a growing concern for protection, where a well executed attack could possibly disrupt several ICT components at once [RBM09] [CDC10].

3.3.3 Geographic Interdependency

Examples of common cause failures caused by a geographic interdependency are flood, fire, explosions or plumes of radioactive gases. Natural disasters, accidents and terrorism are potential initiating events for common cause failures, in which several components in ICT, telecommunication and power grid systems could get damaged at the same time [SOK+13]. Even if smart grid components are not vulnerable to natural disasters themselves, cables and BSs will often be connected to or supported by other infrastructure, like buildings or bridges, which would realistically take damage from earthquakes and other natural disasters [CBK07].

Data from the Swedish national transmission grid shows that six power outages between 1998 and 2003 are due to natural hazards or adverse weather, not including lightning. 89 disturbances are caused due to lightning strikes in the same time span. Weather related failures can be regarded as typical common cause failures, where one natural event, e.g. a thunderstorm or hurricane, could cause several smart grid components located in the same geographical area to fail [HM06].

3.4 Summary

Considering the investigation interdependencies and failures presented, Table 3.1 shows a summary of literature studied categorized along the dimensions of type of dependency and type of failure. From the preceding sections and Table 3.1 it is implied that some scenarios are more relevant than others, for instance that in

Table 3.1: Summary of literature studied in the investigation of failures and interdependencies relevant for smart grids.

	Physical	**Cyber**	**Geographic**
Cascading	[BN03] [BPP+10] [ASC12]	[LKK07] [RBM09]	[SOK+13]
Escalating	...	[LKK07] [KB09] [PSO04]	...
Common	[FRS07] [FH11]	[CDC10] [RBM09]	[CBK07] [SOK+13] [HM06]

the case of geographic failures, the common cause type of interdependency is more dominating than the other types of interdependency. This observation gives an incentive to lay focus on certain scenarios that will affect smart grids the most, namely the scenarios that falls inn under the combinations of interdependencies and failures marked in Table 3.1 with yellow. Because of their relevancy, these four combinations of interdependencies and failures are studied in more details in Part II.

Part II

Interdependency Modeling

Chapter 4
System Description

The system used in this analysis is a specific digital ecosystem, a smart grid. The system is shown in Figure 4.1, and illustrates how power transmissions and power grid monitoring in a smart grid could function. In the smart grid data is gathered by smart units (SUs) and transferred to a control center owned by a power utility company intending to administer the smart grid. For the communication with the SUs there are several alternatives for platforms, which could be chosen depending on requirements concerning latency, availability and security. Investigated in the following is a solution based on mobile communication, an interesting candidate because of relatively low entry costs and roll-out time. The smart grid system is looked at from a single SU's perspective, hence the service is considered as working if the SU is connected to and can communicate with the power utility company's control center.

To sustain a connection between the SUs and the control center the smart grid utilizes mobile communication provided by two MNOs, namely MNO A and MNO B. The easiest and cheapest communication solution would be for each SU to have a subscriber identity module (SIM) belonging to one of the two MNOs, allowing the SU to communicate through only the one MNO owning the SIM. To achieve a more stable connection between the SUs and the control center, the SUs could apply *multihoming*, in which case the SUs will use two SIM cards, one for each MNO, and thus be able to communicate through either. Even with multihoming the SUs can only have a connection through one of the MNOs at the time, where the MNO currently in use is called the *active MNO*.

If a communication failure is detected at the SU, defined as loss of connection with the control center, the SU initiates a switch-over to the other non-active MNO and resume operation given that a connection to the control center can be re-established over this mobile network. If the SU can not establish a connection over either MNO the switch-over is repeated back and forth until the smart grid is repaired and the SU can establish a connection to the control center anew.

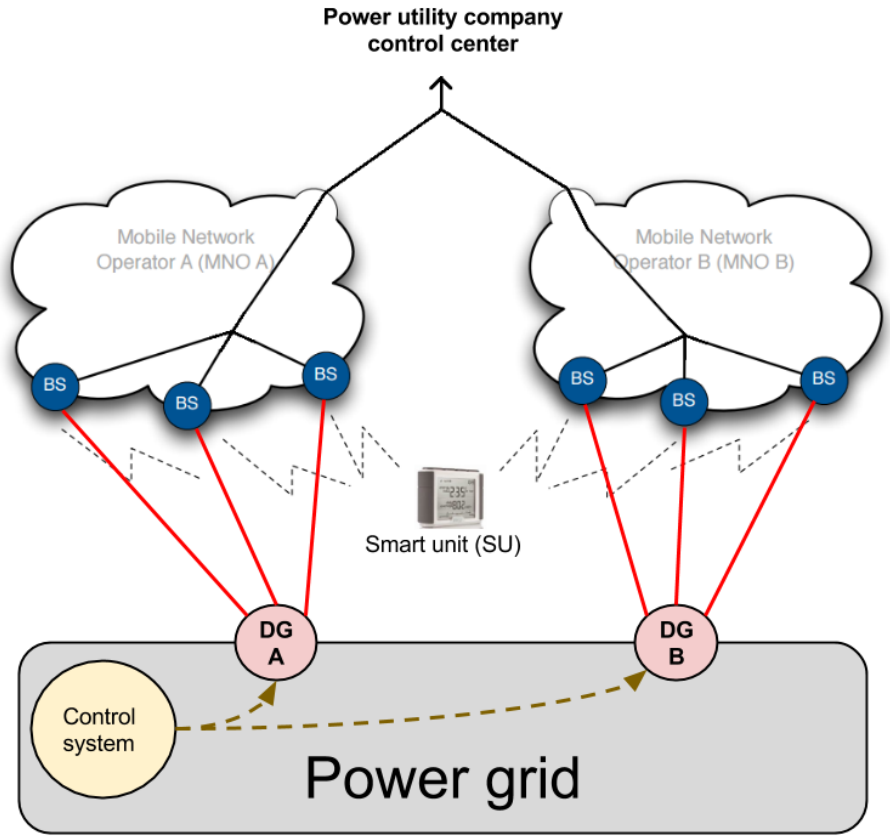

Figure 4.1: The smart grid system analysed including a smart unit, a power grid with two distribution grids, a power grid control system and two MNOs.

A working connection between the SU and the control center relies on six BSs, with three BSs owned by each MNO. The BSs are regarded as working as long as they are operating and able to receive data from the SU and forward this data further on towards the power utility company's control center. To do this the BSs need to be provided with power, either directly from the power grid or from a local power backup, they need to have available bandwidth capacity, and critical hardware (HW) and SW in the BS will have to function correctly.

The BSs rely on power provided by a power grid logically separated into two distribution grids (DGs); DG A is providing the BSs in MNO A with power and DG B is providing the BSs in MNO B with power. All the physical power dependencies

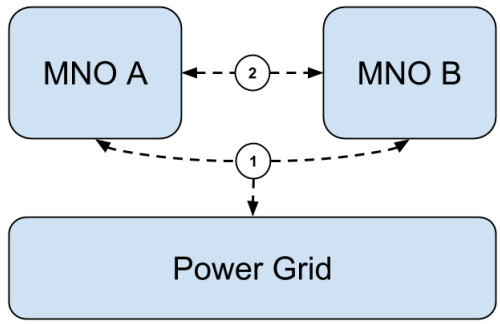

Figure 4.2: Illustration of the two areas of interdependencies; (1) between the power grid and the MNOs and (2) between the two MNOs.

from the BSs to the DGs are shown in Figure 4.1 as red connections. Also, there is a power grid control system monitoring the power grid. If working correctly and having adequate information about the power grid's status, the control system will be able to locate malfunctions and assist any repair personnel in case of DG failures.

4.1 Areas of Interdependencies

The interdependencies that could exist in the smart grid from Figure 4.1 are in this analysis categorised into two areas of interdependencies. In the following analysis each area of interdependency is investigated separately, emphasising the different effects that dependencies have on the two areas of the smart grid individually. The two areas of interdependencies are listed below, and are also illustrated in Figure 4.2.

1. Interdependencies between the power grid and the MNOs.
2. Interdependencies between the two MNOs.

4.2 Values of Rates and Constants

Several use cases are presented and analysed in the following chapters. The numerical values of all rates and constants used in the following analyses are assumed to be exponentially distributed, and are listed in summary in Table 4.1. The rates and constants are explained further in the use cases where they are involved. The DG failure and repair rates are derived from Norwegian power grid interruption statistics [AFÅ+14], while the rest of the values are estimated based on study of literature.

Table 4.1: Values of all rates and constants used in the following use cases.

Use case	Symbol	Value	Explanation
1	λ_{DG}	4/year	Failure rate of the DGs.
	μ_{DG}	1/3h	Repair rate of the DGs.
	λ_{PB}	1/4h	BS power backup run out rate.
	s_{DG}	1.5	Constant for realising DG stress propagation.
	c_{DG}	0.5	Constant for realising inadequate telecom.
2	λ_C	5/year	Congestion rate of the BSs.
	μ_C	1/4h	Congestion repair rate of the BSs.
	l_{BS}	30	Constant for realising congestion propagation.
3	λ_{Er}	24/year	BS malware infection rate.
	μ_{Er}	3/year	SW repair rate of BSs in error state.
	λ_F	12/year	SW failure rate of malware infected BSs.
	μ_F	1/7h	SW repair rate of failed BSs.
	m_{BS}	2.5	Constant for realising malware propagation.
4	λ_{CS}	5/year	Failure rate of the power grid control system.
	μ_{CS}	1/7h	Repair rate of the power grid control system.
	m_{CS}	2/3	Constant for realising escalated repair time.
	+ λ_{DG}, μ_{DG}, λ_{PB}, s_{DG} and c_{DG} from use case 1.		
5	λ_S	3/year	Rate of BS damaging storms.
	λ_W	2/year	Failure rate of BS because of weathering.
	μ_{BS}	1/10h	Repair rate of failed BSs.
	P_S	1/6	Probability of a BS failing in a storm.
6	λ_D	3/year	Damage rate of ditch with BS power cables.
	μ_D	2/15h	Repair rate of ditch with BS power cables.
	+ λ_W and μ_{BS} from use case 5.		

Chapter 5
Use Cases - Introduction

Based on the investigation from Chapter 3 it is understood that several types of dependencies can exist and different types of failures can occur in each area of interdependencies. To further analyse how dependencies and failures behave in and affect the smart grid some distinct use cases are made, which are presented in this chapter, and will be analysed one at a time in the following chapters.

From Table 3.1 in Chapter 3 some combinations of interdependencies and failures where pointed out as the most relevant for smart grids. The following use cases are chosen based on this observation, and covers the presumably most realistic and relevant scenarios. Because of this, only some of the types of interdependencies and types of failures are investigated for each of the two areas of interdependencies, creating in all six distinctive use cases.

In each use case a specific type of failure, a specific type of interdependency and a specific areas of interdependency is analysed. More precisely, the availability of the smart grid system is analysed for each of the use cases through the use of dependability modeling. To model the dependability of the system concerned, Markov processes represented by state transition diagrams are used, also known as, and in the following chapters referred to as, *Markov dependability models*. By using Markov dependability models the *asymptotic availability* of the smart grid system can be obtained in each use case, and ultimately be compared with the asymptotic availabilities obtained in other use cases. For more information on Markov dependability models see [Hel09] or [EHHP12], where in the following chapters the reader is assumed to have basic knowledge of notations and topology in dependability modeling.

The use cases all build up step by step by first introducing a simple system, then adding dependencies to the system and in this way increasing complexity. This way of presenting the use cases allows the asymptotic availability as well as the actual Markov dependability models of the smart grid system to be compared when various dependencies are added. Each use case will to sum up present a discussion, analysing

the most important parameters in that use case and how they affect the asymptotic availability of the smart grid. In addition, a final discussion is presented after the use cases, looking at the dependability models presented and comparing the numerical results from the use cases.

The six use cases presented, modeled and analysed in the following chapters are summarised in the list below. Table 5.1 sum up the area of interdependency, the type of failure and the type of interdependency that are concerned in each use case

Use Case 1: Cascading Power Grid Failure
This use case presents a scenario where a DG in the power grid fails and causes propagation of failure in the power grid. The failure(s) in the power grid will further on cascade and cause a blackout in the BSs in the MNOs.

Use Case 2: Cascading Base Station Congestion Failure
All BS has a set bandwidth capacity, where if a BS experiences too much load it will become congested. This use case investigates how BS congestion can propagate between BSs in an MNO or cascade to BSs in the other MNO.

Use Case 3: Cascading Base Station Cyber Failure
This use case analyse how malware can infect and propagate between BSs in a MNO, or cascade between BSs in different MNOs.

Use Case 4: Escalating Cascading Power Grid Failure
If the power grid control system is failed, potential failures in the power grid will be more severe in the form of a longer repair time. This use case is similar to Use Case 1, though with the addition of a power grid control system.

Use Case 5: Common Cause BS Failure with Individual Repair
A storm may potentially cause damage to several BSs in a geographical area at once. This use case investigates how a storm could cause a common cause BS failure in the MNOs.

Use Case 6: Common Cause BS Failure with Common Repair
This use case also investigates a common cause failure, more specifically the damaging of a ditch containing BS power cables. Here only the ditch has to be repaired for the BSs to work, not every BSs individually.

Table 5.1: Overview of use cases analysed.

Use case	Area of interdependency	Type of failure	Type of interdependency
1	1	Cascading	Physical
2	2	Cascading	Physical
3	2	Cascading	Cyber
4	1	Escalating	Cyber
5	2	Common cause	Geographical
6	2	Common cause	Geographical

Chapter 6
Use Case 1: Cascading Power Grid Failure

From the investigation in Section 3.1 it is seen that there are several ways in which components can fail and start a propagation of disruptions throughout a network. In the case of power grids, transmission lines and other HW components could fail due to overload, decay and flashovers among other reasons, starting a ripple effect of power grid components failing.

A DG in the smart grid system from Figure 4.1 is defined as failed when critical components in the DG have failed and the DG can no longer provide power to its dependent BSs. In the same way as disruptions propagate in a network when components fail, stress will propagate between the DGs in the power grid. Additional stress on a DG does not necessarily cause it to fail, but will increase the chance of it failing due to overload. In this use case, if DG A fails stress is increased on DG B, and vice versa, if DG B fails stress is increased on DG A. Implicitly, besides failures propagating in the power grid, a failure can cascade from the power grid to other systems. As the BS in the MNOs rely on power from the power grid, they will fail if the DGs on which they rely fails, if not having backup power of some kind.

Different factors affect the failure and repair rates of the DGs and how fast failures could cascade from the power grid to the MNOs, where MNO failures contrarily can affect the state of the power grid. Figure 6.1 illustrates the chronological steps of how a failure cascade and affect the power grid and the MNO systems in the smart grid from Figure 4.1. The steps from Figure 6.1 are gone through and explained further in the following sections.

6.1 Cascading Power Grid Failure

In the simplest form the smart grid system is assumed to work such that the BSs in the MNOs have no power backup and does not fail due to any other causes than lack of power. A failure of DG A or DG B will immediately cascade to the BSs in MNO A or MNO B respectively, causing them to fail.

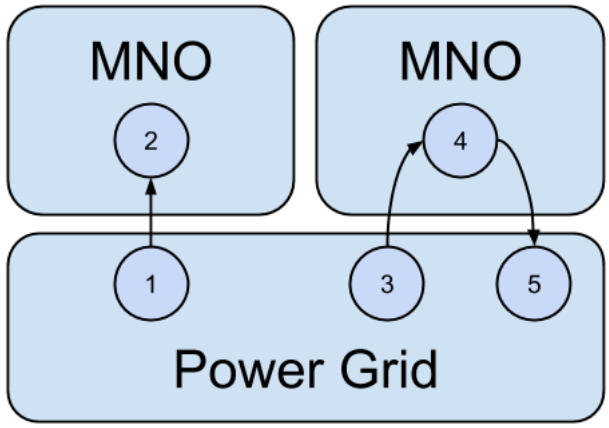

Figure 6.1: Steps of a cascading failure starting in the power grid; (1) failure of a DG, (2) failure of BSs in an MNO due to power outage, (3) failure of a second DG, (4) failure of BSs in a second MNO due to power outage, and (5) DG repair time increases.

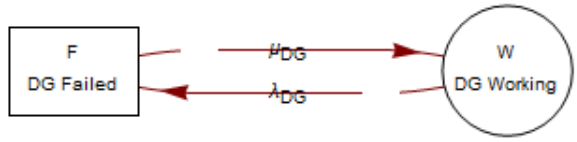

Figure 6.2: Markov dependability model of a single DG system.

6.1.1 Single Distribution Grid Dependency

For the sake of comprehension, a more simple system is presented first. Assuming the SU only has one SIM card, the SU can only connect to BSs belonging to one of the MNOs. The failure of a single DG is seen in Figure 6.1 as the first step, (1) failure of a DG. When the one DG in this simple system without SU multihoming fails, the failure cascades to the dependent BSs. The failure of BSs in a single MNO is seen in Figure 6.1 as the second step, (2) failure of BSs in an MNO.

In this dependability model only one of the DGs has to be regarded, The DG powering the one active MNO. The state space is defined as $\Omega = \{\text{DG Working, DG Failed}\}$. Knowing the failure rate λ_{DG} and the repair rate μ_{DG} of the DG, the dependability model becomes as seen in Figure 6.2.

With the steady state probabilities from the dependability model in Figure 6.2, denoted $\underline{p} = \{p_W, p_F\}$, the asymptotic availability A_{DG} of the DG system equals the

Figure 6.3: Markov dependability model of the smart grid system from Figure 4.1 including stress propagation between DGs.

steady state probability of the one working state, as shown in (6.1).

$$A_{DG} = p_W = 0.998632 \tag{6.1}$$

6.1.2 Power Grid Dependency

With multihoming the SU in the smart grid system can connect to both MNOs. The failure of the first DG is seen in Figure 6.1 as the first step, (1) failure of a DG. When the first DG fails the failure cascades to its dependent BSs, seen as the second step, (2) failure of BSs in an MNO. The failure of the second DG is seen as the third step, (3) failure of a second DG, which again cascades and causes the BSs in the second MNO to fail, seen as step four, (4) failure of BSs in a second MNO.

When both DGs are included in the dependability model the propagating of stress between them will also have to be regarded, realized with a DG stress constant s_{DG}. If a DGs fails, the failure rate of the other DG is increased with s_{SG} and becomes $(1 + s_{DG})\lambda_{DG}$. In this dependability model the state space is defined as $\Omega = \{\{i\text{DG Working}\} \mid i \in \{0, 1, 2\}\}$, where the system is defined as working when at least one DG is working. Assuming there is only one repair crew in the power grid, knowing the failure rate λ_{DG} and the repair rate μ_{DG} of the DGs and including the stress propagation between the DGs, the dependability model becomes as seen in Figure 6.3.

With the steady state probabilities from the dependability model in Figure 6.3, denoted $\underline{p} = \{p_1, p_2, p_3\}$, the asymptotic availability A_{SG} of the smart grid system is obtained by adding up the steady state probabilities of the working states, as shown in (6.2).

$$A_{SG} = p_1 + p_2 = 0.999991 \tag{6.2}$$

Figure 6.4: Markov dependability model of the smart grid system from Figure 4.1 including stress propagation between DGs and repair crew telecommunication dependency.

6.1.3 Power Grid & MNO Interdependency

Not only can the power grid affect the states of the BSs in the MNOs, but the failure of the BSs can disrupt the state of the power grid. The DG repair crew is assumed to use the telecommunication services provided by the MNOs for communication between personnel and coordination of repair operations, therefore when all BSs have failed the DG repair work will be somewhat slowed. The failure of the first DG is seen in Figure 6.1 as the first step. When the first DG fails the failure cascades to its dependent BSs, seen as the second step. The failure of the second DG is seen as the third step, which again cascades and causes the BSs in the second MNO to fail, seen as step four. Lastly, when all BSs has failed the power grid repair crew becomes in lack of proper telecommunication services, seen as step five, (5) DG repair time disruption.

The potential decrease in DG repair rate is realized with a communication constant c_{DG}. If both DGs have failed and all BSs are without power, the repair rate of the DGs are decreased with c_{DG} and becomes $(1 - c_{DG})\mu_{DG}$. The dependability model for this system again relies on only the two DGs, giving it the same state space as in the model from Section 6.1.2, defined as $\Omega = \{\{i\text{DG Working}\} \mid i \in \{0, 2\}\}$. The system is defined as working when at least one DG is working, and it is assumed that there is only one repair crew in the power grid. Knowing the failure rate λ_{DG} and the repair rate μ_{DG} of the DGs, including the stress propagation between the DGs, and including the repair crew telecommunication dependency, the dependability model becomes as seen in Figure 6.4.

With the steady state probabilities from the dependability model in Figure 6.4, denoted $\underline{p} = \{p_1, p_2, p_3\}$, the asymptotic availability A_{SG} of the smart grid system is obtained by adding up the steady state probabilities of the working states, as shown in (6.3).

$$A_{SG} = p_1 + p_2 = 0.999981 \tag{6.3}$$

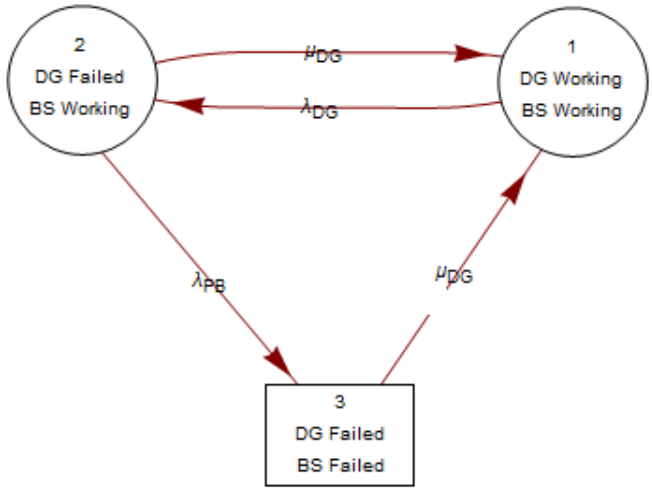

Figure 6.5: Markov dependability model of a single BS system.

6.2 Cascading Power Grid Failure with BS Power Backup

BSs in a real system will often have power backup of some kind, e.g. diesel generators or batteries [Mal10]. When including power backup for the BSs in the smart grid system there will be an extra delay between the moment a DG fails and the moment its dependent BSs fails. This means that the smart grid asymptotic availabilities obtained from (6.2) and (6.3) are too low if the BSs have power backup. The BSs in this section are assumed to not fail for any other reason than lack of power and the power run out rate for the BSs is assumed to be exponentially distributed as the capacity of diesel generators and batteries can vary based on type, age, working conditions and state of charge.

6.2.1 Single Base Station Dependency

First assuming the SU can only connect to a single BS, a simple dependability model illustrating the cascading of failure from a DG to the single BS can be made. The state space is in this model two dimensional, defined as $\Omega = \{\{i\text{DG Working}, j\text{BS Working}\} \mid i \in \{0,1\}, j \in \{0,1\}, j \geq i\}\}$, including both the state of the DG and the state of the BS. For the single BS system to fail the DG powering the BS has to fail and the BS has to run out of power backup, where the BS power backup is assumed to run out with rate λ_{PB}. The DG failures are assumed to happen rarely enough for the BS power backup to recharge between DG failures. Knowing the failure rate λ_{DG} and the repair rate μ_{DG} of the DGs and the BS backup power run out rate λ_{PB}, the dependability model becomes as seen in Figure 6.5.

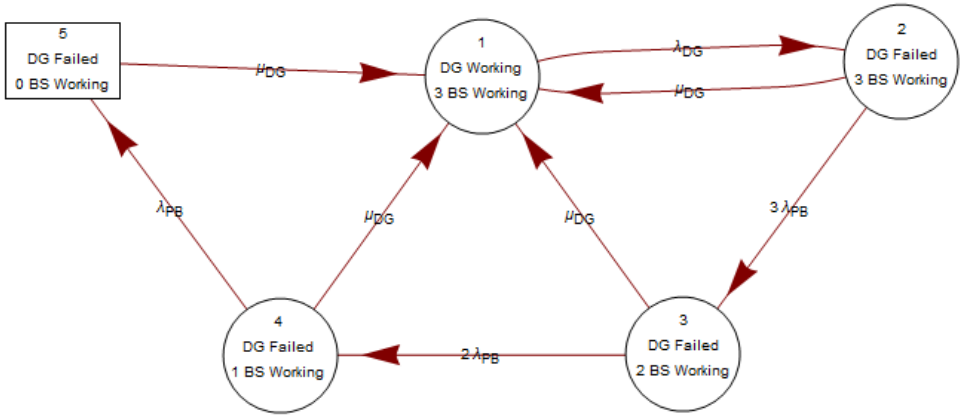

Figure 6.6: Markov dependability model of a single MNO system including BS power backup.

With the steady state probabilities from the dependability model in Figure 6.5, denoted $\underline{p} = \{p_1, p_2, p_3\}$, the asymptotic availability A_{BS} of the single BS system is obtained by adding up the steady state probabilities of the working states, as shown in (6.4).

$$A_{BS} = p_1 + p_2 = 0.999414 \tag{6.4}$$

6.2.2 Single Distribution Grid Dependency

Assuming the SU only has one SIM card, the SU can only connect to BSs belonging to one of the MNOs. The failure of a single DG is seen in Figure 6.1 as the first step, (1) failure of a DG. When the one DG in this simple system without SU multihoming fails, the failure cascades to the dependent BSs. The failure of BSs in a single MNO is seen in Figure 6.1 as the second step, (2) failure of BSs in an MNO.

Here only one of the DGs has to be regarded in the dependability model, the one powering the applicable MNO. A new dependability model is made extending the model from Figure 6.5, where instead of only one BS there are three BSs included in the model. The state space for this single MNO system is defined as $\Omega = \{i\text{DG Working}, j\text{BS Working}\} \mid i \in \{0,1\}, j \in \{0,1,2,3\}, j \geq 3i\}$. In this single MNO system the DG has to fail and all three BSs has to run out of power before the MNO system fails, each BS with power run out rate λ_{PB}. Knowing the failure rate λ_{DG} and the repair rate μ_{DG} of the DGs, the dependability model becomes as seen in Figure 6.6.

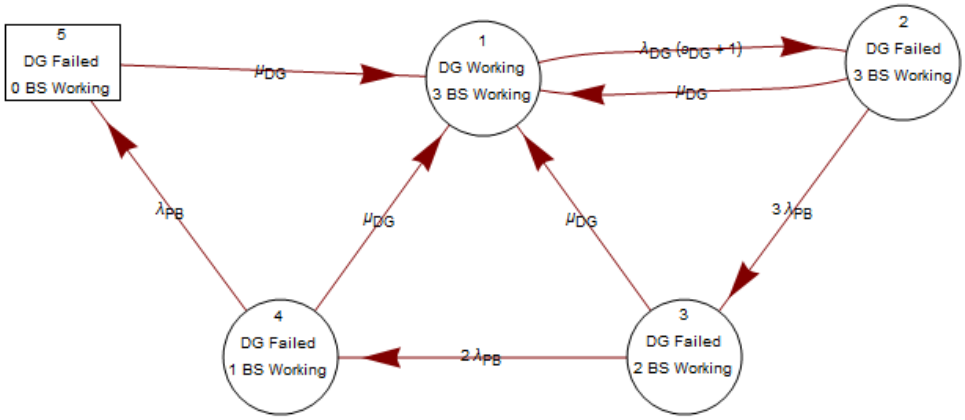

Figure 6.7: Markov dependability model of a single MNO system including BS power backup with increased DG stress.

With the steady state probabilities from the dependability model, denoted $\underline{p} = \{p_1, p_2, p_3, p_4, p_5\}$, the asymptotic availability A_{MNO} of the MNO system is obtained by adding up the steady state probabilities of the working states, as shown in (6.5).

$$A_{MNO} = p_1 + p_2 + p_3 + p_4 = 0.999756 \tag{6.5}$$

6.2.3 Power Grid Dependency

Now assuming the SU is multihomed and can connect to both MNOs. The failure of the first DG is seen in Figure 6.1 as the first step, (1) failure of a DG. When the first DG fails the failure cascades to its dependent BSs, seen as the second step, (2) failure of BSs in an MNO. The failure of the second DG is seen as the third step, (3) failure of a second DG, which again cascades and causes the BSs in the second MNO to fail, seen as step four, (4) failure of BSs in a second MNO.

As already seen from the dependability models in Figure 6.3 and Figure 6.4, when a DG fails the failure rate of the other DG is increased with a stress constant s_{DG}. This means that if a DG has failed the potentially remaining working DG would have an increased DG failure rate; more specifically the DG failure rate becomes $(1 + s_{DG})\lambda_{DG}$. The dependability model of a DG and all three dependent BSs in the case of increased DG stress is seen in Figure 6.7.

Creating a dependability model of the smart grid covering both DGs and all six BSs is very much possible, but would be a complex model. As an alternative, by

Figure 6.8: Markov dependability model of the smart grid system from Figure 4.1 including stress propagation between DGs and BS power backup.

finding the failure rate of the systems from Figure 6.6 and Figure 6.7, a simpler dependability model for the smart grid system can be made. Denoting the steady state probabilities from the model in Figure 6.7 as $\underline{p_s} = \{p_{1s}, p_{2s}, p_{3s}, p_{4s}, p_{5s}\}$ and using the already denoted steady state probabilities $\underline{p}$ from the dependability model in Figure 6.6, the failure rate λ_{MNO} of the system in Figure 6.6 and the failure rate λ_{MNOs} of the system in Figure 6.7 are obtained in (6.6) and (6.7) respectively.

$$\lambda_{MNO} = \frac{p_4}{p_1 + p_2 + p_3 + p_4}\lambda_{PB} \tag{6.6}$$

$$\lambda_{MNOs} = \frac{p_{4s}}{p_{1s} + p_{2s} + p_{3s} + p_{4s}}\lambda_{PB} \tag{6.7}$$

A dependability model of the smart grid system is made with state space defined as $\Omega = \{i\text{MNO Working}\} \mid i \in \{0, 1, 2\}\}$, including both the DGs and the BSs with power backup. With the failure rates λ_{MNO} and λ_{MNOs} obtained and knowing the repair rate μ_{DG} of the DGs, the dependability model becomes as seen in Figure 6.8.

With the steady state probabilities from the dependability model in Figure 6.8, denoted $\underline{p_{SG}} = \{p_{1sg}, p_{2sg}, p_{3sg}\}$, the asymptotic availability A_{SG} of the smart grid system including stress propagation between DGs and BS power backup is obtained by adding up the steady state probabilities of the working states, as shown in (6.9).

$$U_{SG} = p_{3sg} = 2.96 \times 10^{-7} \tag{6.8}$$

$$A_{SG} = p_{1sg} + p_{2sg} = 1 - U_{SG} \tag{6.9}$$

6.2.4 Power Grid & MNO Interdependency

Including the repair crew telecommunication interdependency, the repair time for the DGs when all BSs have failed will be somewhat increased. With the obtained failure

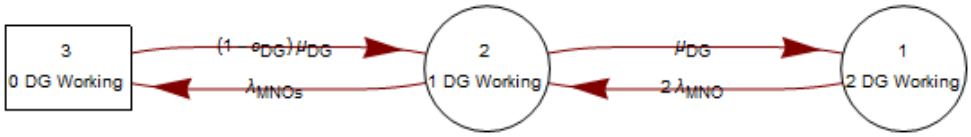

Figure 6.9: Markov dependability model of the smart grid system from Figure 4.1 including stress propagation between DGs, repair crew telecommunication dependency, and BS power backup.

rates for the MNO systems, Λ_{MNO} and Λ_{MNOs}, a new dependability model of the smart grid system including the repair crew telecommunication interdependency is easily obtained.

For the new model of the smart grid the only rate changing from the model in Figure 6.8 is the repair rate from the failed state, which will be decreased by the communication constant c_{DG}. The state space of this new model is defined as $\Omega = \{i\text{MNO Working}\} \mid i \in \{0, 2\}\}$, giving the model as seen in Figure 6.9.

With the steady state probabilities from the dependability model in Figure 6.9, denoted $p_{SG} = \{p_{1sg}, p_{2sg}, p_{3sg}\}$, the asymptotic availability A_{SG} of the smart grid system including stress propagation between DGs, repair crew telecommunication dependency, and BS power backup is obtained by adding up the steady state probabilities of the working states, as shown in (6.10).

$$A_{SG} = p_{1sg} + p_{2sg} = 0.999999 \tag{6.10}$$

6.3 Discussion

With the dependability models created for the smart grid systems with or without multihoming, repair crew telecommunication dependency and BS power backup, a comparison of the systems with regard to asymptotic availability can be made. First the systems from Section 6.1 are compared, being the smart grid systems without BS power backup. From Norwegian power grid interruption statistics it is seen that there is an evident variation of power grid failure rate among Norwegian counties, and on this wise the failure rate of the systems is looked at [AFÅ+14]. The plot in Figure 6.10 shows the asymptotic availability of the systems from Figure 6.2, Figure 6.3 and Figure 6.4 plotted with respect to DG failure rate λ_{DG}.

It is seen from the plot in Figure 6.10 that the single DG system has a notably steeper decrease in asymptotic availability than the two other systems as the failure

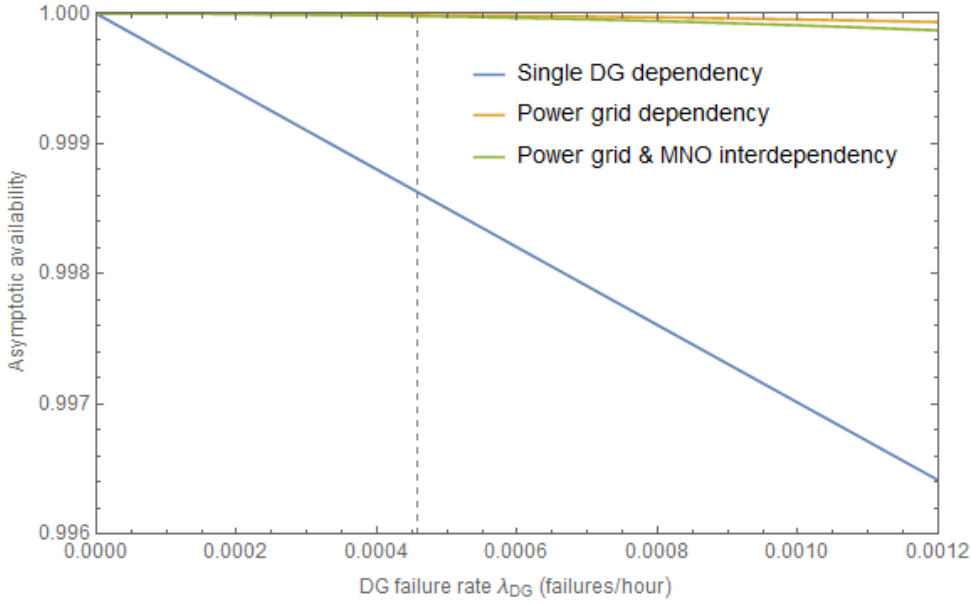

Figure 6.10: Plot of the asymptotic availability of the three smart grid systems from Figure 6.2, Figure 6.3 and Figure 6.4 with respect to DG failure rate λ_{DG}. The dashed grid line shows the value of the DG failure rate λ_{DG} used in use case 1.

rate λ_{DG} increases, going up to almost one DG failure every month. The asymptotic availability of the two other smart grid systems stays approximately the same in the failure rate range given, implying that the telecommunication repair crew dependency as realised in this analysis does not have a significant effect on the smart grid's asymptotic availability.

Because the asymptotic availability of the systems from Figure 6.3 and Figure 6.4 stays relatively high with regard to increasing failure rate, comparing them to the corresponding systems from Section 6.2 with BS power backup would give little useful insight. For the two systems with only one DG, with and without BS power backup, a more notable distinction can be seen. The plot in Figure 6.11 shows the asymptotic availability of the two single DG systems from Figure 6.2 and Figure 6.6 plotted with respect to BS power backup run out rate λ_{PB}.

With a four hour mean time to BS power backup run out, shown in the plot in Figure 6.2 as a dashed grid line, the effect of the BS power backup is noteworthy, but quickly loses effect as λ_{PB} increases. The asymptotic availability of the single DG system with BS power backup will eventually converge to the asymptotic availability of the single DG system without BS power backup as λ_{PB} approaches infinity. To

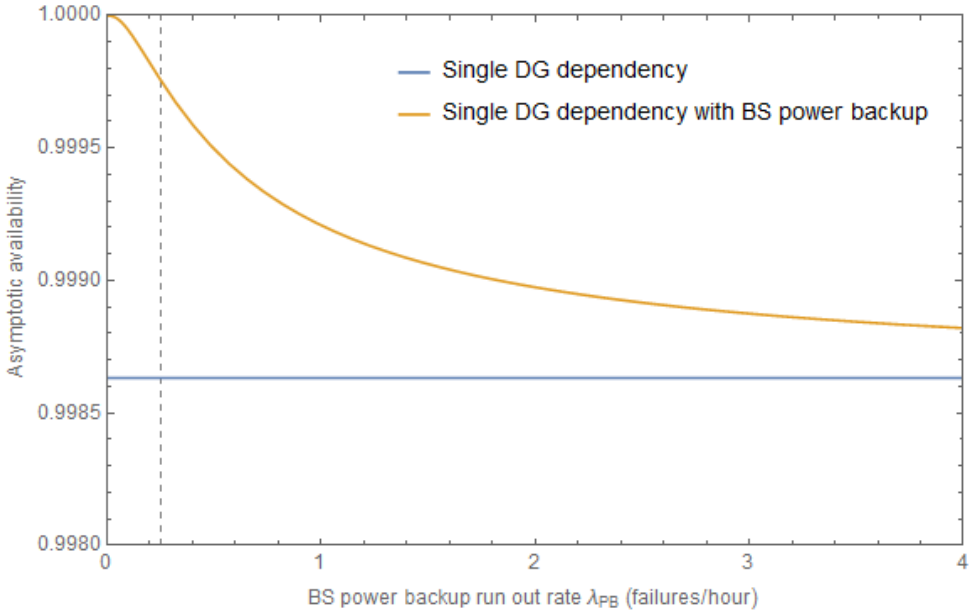

Figure 6.11: Plot of the asymptotic availability of the two single DG systems from Figure 6.3 and Figure 6.4 with respect to BS power backup run our rate λ_{PB}. The dashed grid line shows the value of the BS power backup run our rate λ_{DG} used the use case 1.

uphold an adequate effect of the BS power backup in case of a single DG system, the BS power backup should last no less than a couple hours.

Going back to the multihomed systems with two DGs, the effect of the BSs power backup becomes more evident if the communication constant c_{DG} is increased. The plot in Figure 6.12 shows the asymptotic availability of the two systems from Figure 6.3 and Figure 6.9 plotted with respect to c_{DG}. As seen from the plot, when c_{DG} is increased, the smart grid system without BS power backup will have a significant decrease in asymptotic availability before there is a big change in the asymptotic availability of the smart grid system with BS power backup. This suggests that for areas without alternative telecommunication services a better power backup solution is more important.

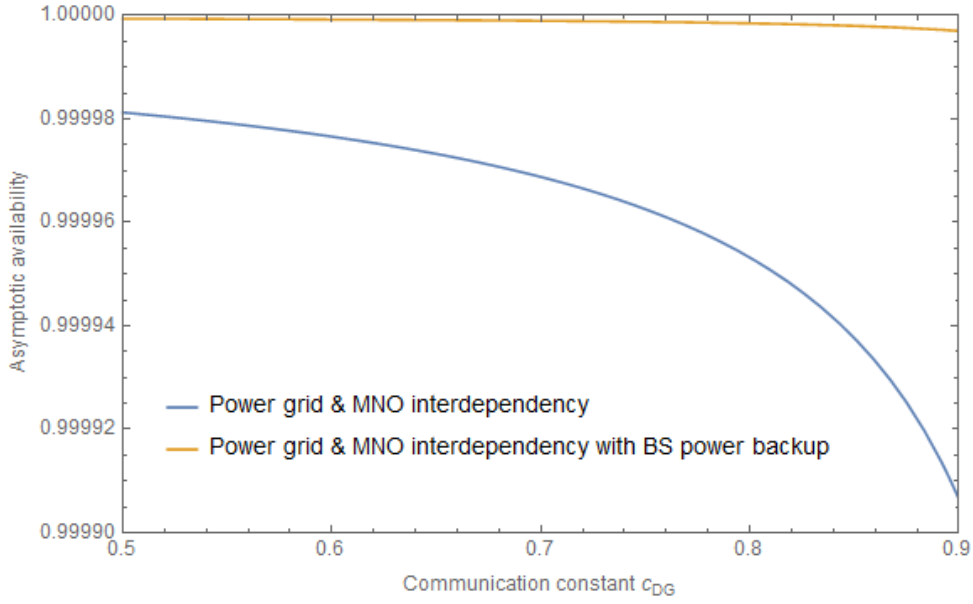

Figure 6.12: Plot of the asymptotic availability of the two smart grid systems from Figure 6.3 and Figure 6.9 with respect to the communication constant c_{DG}.

Chapter 7
Use Case 2: Cascading Base Station Congestion Failure

BSs could become erroneous if experiencing a high amount of load, and in the worst case not being able to receive and communicate calls and data from the SUs and other users due to bandwidth capacity. User crowding in areas related to popular events, increased data traffic due to emergency situations, or BS failures causing higher load on remaining working BSs in a geographical area are all examples of scenarios where BS overloads could occur [BCH+12] [Ald03] [Mei12]. In the smart grid system from Figure 4.1, when a BS in an MNO experiences an overload and is no longer available for new requests, the remaining BSs in that MNO has to take all load, and thus are more subjected to overload themselves. In this way overload failures in BSs propagate to other BSs in their system, or even to other systems, in this case the other MNO, if users and SUs have access to both MNOs.

In the following sections the BSs can be in a normal (working) state or in a congested (failed). In the congested state the BS can handle no extra load, and all load is therefore redistributed to other BSs if possible, including SU requests. Figure 7.1 illustrates the chronological steps in which a BS congestion failure in an MNO can propagate to other BSs in the MNO, cascade to the other MNO, and again cascade back realizing a BS interdependency between the MNOs. The steps from Figure 7.1 are explained further in the following sections.

7.1 Single BS Congestion

For the sake of comprehension, first the SU is assumed to only be able to connect to a single BS. The congestion of a single BS is seen in Figure 7.1 as the first step, (1) congestion of a BS in an MNO, and the BS is assumed not to fail for any other reasons than BS congestion. The rate of which the BS becomes congested is assumed to be λ_C, where the BSs are assumed to do self-restore by reboot, remote configuration or by change of situation (e.g. decreasing demand) in the case of congestion, giving the BSs an independent restoration rate of μ_C. The state space of the single BS

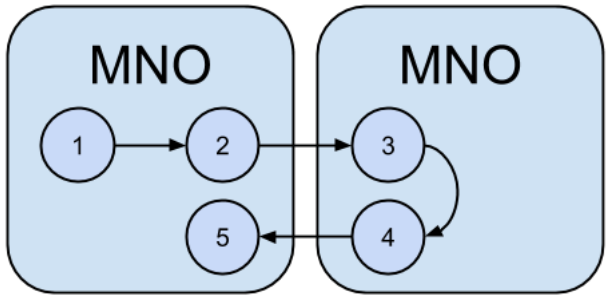

Figure 7.1: Steps of a cascading BS congestion failure; (1) congestion of a BS in an MNO, (2) propagation of BS congestion in an MNO, (3) cascading of BS congestion to a second MNO, (4) propagation of BS congestion in a second MNO, and (5) cascading of BS congestion back to the first MNO.

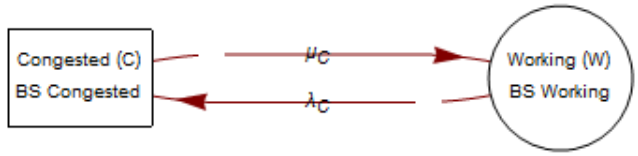

Figure 7.2: Markov dependability model of a single BS system with congestion.

system is defined as $\Omega = \{\text{BS Working, BS Congested}\}$, and knowing the BS failure and restoration rates a simple dependability model of a single BS system can be made as seen in Figure 7.2.

With the steady state probabilities from the dependability model in Figure 7.2, denoted $\underline{p} = \{p_W, p_C\}$, the asymptotic availability A_{BS} of the single BS system is simply the one working steady state probability, as shown in (7.1).

$$A_S = p_W \tag{7.1}$$

7.2 Propagating BS Congestion

Assuming the SU only has one SIM card, it can only connect to BSs belonging to one of the MNOs. It is assumed that the BSs do not fail for any other reason than congestion. Because there are several BSs in a single MNO, propagation of BS congestion between the BSs in that MNO has to be taken into account when analysing the system. The congestion of a single BS is seen in Figure 7.1 as the first step, (1) congestion of a BS in an MNO. When a BS is congested it will cause extra

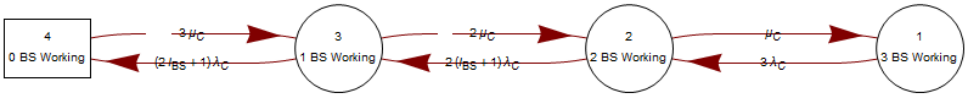

Figure 7.3: Markov dependability model of a single MNO system with congestion propagation.

load on remaining BSs and in this way propagate congestion, seen in Figure 7.1 as the second step, (2) propagation of BS congestion in an MNO.

The rate at which a BS in an MNO experiences congestion and goes to the congested state is λ_C, and the restoration rate is μ_C. When a BS in an MNO is congested it increases the rate at which other BSs in that MNO becomes congested with a load constant l_{BS}, i.e. the congestion rate for remaining normal working BSs in the MNO becomes $(1 + l_{BS})\lambda_C$. Likewise, when two out of three BSs in an MNO are congested the congestion rate for the one last normal working BS in that MNO becomes $(1 + 2l_{BS})\lambda_C$. State space of the single MNO system is then defined as $\Omega = \{\{i\text{BS Congested}\} \mid i \in \{0, 3\}\}$, giving the dependability model as seen in Figure 7.3.

With the steady state probabilities from the dependability model in Figure 7.3, denoted $\underline{p} = \{p_1, p_2, p_3, p_4\}$, the asymptotic availability A_{MNO} of the MNO system with BS congestion propagation can be obtained. The single MNO system is working as long as at least one BS in that MNO is working, giving the system asymptotic availability as seen in (7.2).

$$A_{MNO} = p_1 + p_2 + p_3 = 0.999978 \tag{7.2}$$

7.3 Cascading BS Congestion

To obtain the asymptotic availability of the whole smart grid system from Figure 4.1 with respect to BS congestion, both MNOs and all six BSs have to be regarded. Considering that some user agents are multihomed and can utilize BSs from both MNOs, BS overload can cascade between the MNOs. Examples are SUs, other multihomed services or people making emergency calls. Also, the BSs are assumed to have a geographical interdependency, meaning that a crowding of users in an area affecting one of the MNOs' BSs increase the probability that crowded users will affect the other MNO's BSs as well.

7.3.1 MNO Congestion Dependency

The congestion of the first BS is seen in Figure 7.1 as the first step, (1) congestion of a BS in an MNO. When a BS is congested it will cause extra load on remaining BSs and in this way propagate congestion inside the MNO, seen in Figure 7.1 as the second step, (2) propagation of BS congestion in an MNO. Also, BS congestion will cascade to the second MNO seen in Figure 7.1 as the third step, (3) cascading of BS congestion to a second MNO. If at least one BS fails in the second MNO, congestion will also propagate between BSs in this MNO, seen as the fourth step, (4) propagation of BS congestion in a second MNO.

Assuming that the probability of congestion cascading from BSs in one MNO to another increase as more BSs in an MNO are congested. Looking at the dependability model of a single MNO system from Figure 7.3, BS congestion is cascaded from an MNO when the MNO is any state except the first state, where no BSs are congested. It is assumed that there is a higher threshold for cascading congestion from a BS to a BS in another MNO than propagating congestion to a BS belonging to the same MNO. For each congested BS in an MNO there is an increase in congestion rate with a half load constant $\frac{1}{2}l_{BS}$ of BSs belonging to the other MNO. Thus, again looking at the dependability model in Figure 7.3, the congestion rate of BSs belonging to the other MNO is increased with $\frac{1}{2}l_{BS}$, $\frac{2}{2}l_{BS} = l_{BS}$ or $\frac{3}{2}l_{BS}$ when in system state 2, state 3 or state 4 respectively.

Knowing the steady state probabilities from the dependability model in Figure 7.3 a mean congestion rate increase for the second MNO can be obtained. By adding all congestion rate increases l_{BS} multiplied with the steady state probability of the state in which they occur, a mean congestion rate increase L_{BS} for the second MNO is obtained, as seen in (7.3).

$$L_{BS} = (\frac{1}{2}p_{S2} + p_{S3} + \frac{3}{2}p_{S4})l_{BS} \tag{7.3}$$

With the mean congestion rate increase for the second MNO obtained, a new MNO dependability model can be made with the extra congestion rate increase. For all congestion rates the constant L_{BS} is added, giving the dependability model as seen in Figure 7.4.

The smart grid system including both MNOs and BS congestion cascading from one MNO to the other is working as long as at least one of the six BSs is working. Using the steady state probabilities $\underline{p}$ from the system in Figure 7.3, and denoting the steady state probabilities from the system in Figure 7.4 as $\underline{p_l} = \{p_{1l}, p_{2l}, p_{3l}, p_{4l}\}$,

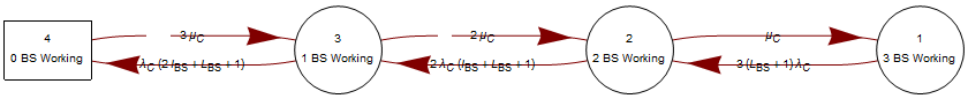

Figure 7.4: Markov dependability model of a single MNO system with congestion propagation including cascading of congestion from the other MNO.

the smart grid system's asymptotic availability A_{SG} can be seen in (7.5).

$$U_{SG} = p_{S4} p_{S_l 4} = 5.60 \times 10^{-10} \tag{7.4}$$

$$A_{SG} = 1 - U_S \tag{7.5}$$

7.3.2 MNO Congestion Interdependency

If BS congestion can cascade from one MNO to another, it will realistically cascade the other way around as well, creating an interdependency between the MNOs. The probability of an MNO being in a state where it can cascade BS congestion is bigger when the MNO can experience cascaded congestion from the other MNO, and thus the probability for cascading congestion back gets bigger as well, enlarging the mean congestion rate increase L_{BS}. This interdependency with BS congestion cascading back to the first MNOs is seen as step five in Figure 7.1, (5) cascading of BS congestion back to the first MNO.

To get a probability for BS congestion cascade as precise as possible the constant L_{BS} has to be recalculated repeatedly until it converges to some value. The recalculation of L_{BS} is a manageable task with a mathematical tool, and the new numerical value for L_{BS} is seen in (7.6).

$$L_{BS} = 0.132998 \tag{7.6}$$

Using the numerically obtained congestion rate increase L_{BS} and the dependability model from Figure 7.4, the asymptotic availability A_{SG} for the smart grid system including MNO interdependency in the form of BS congestion cascading is obtained, as seen in (7.8).

$$U_S = P_{S_l 4}^2 = 6.48 \times 10^{-10} \tag{7.7}$$

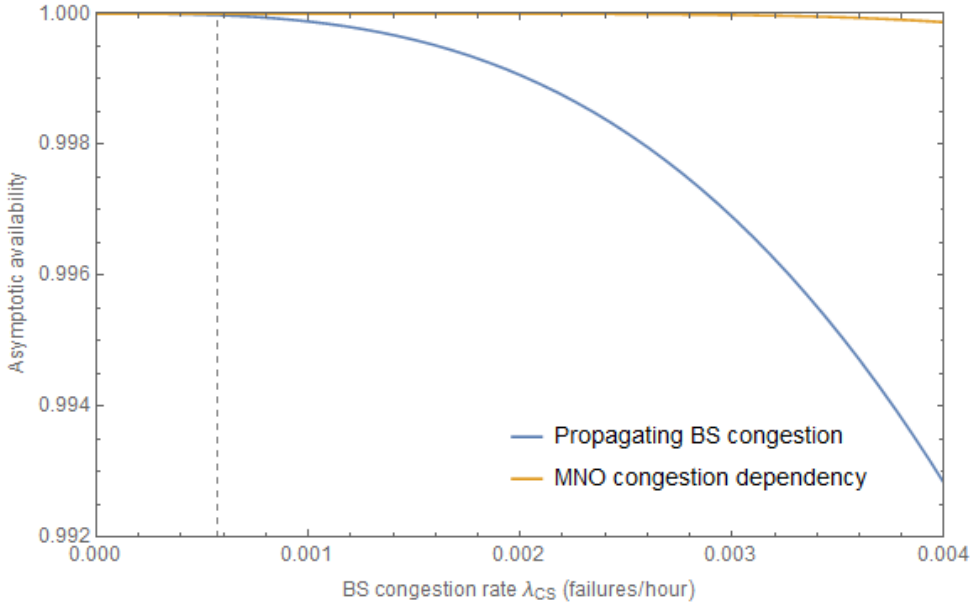

Figure 7.5: Plot of the asymptotic availability of the two smart grid systems from Figure 7.3 and Figure 7.4 with respect to BS congestion rate λ_C. The dashed grid line shows the value of the BS congestion rate λ_C used in use case 2.

$$A_S = U_S \tag{7.8}$$

7.4 Discussion

With dependability models created for the MNO systems with BS congestion some observations are made. In a multihomed system with two MNOs the asymptotic availability stays positively high, both when including congestion dependency and interdependency. On that remark, it is more interesting to look at the single MNO system with congestion propagation, where the asymptotic availability is noticeably lower than for the multihomed systems. The plot in Figure 7.5 shows the asymptotic availability of the single MNO system from Figure 7.3 and the multihomed system from Figure 7.4 plotted with respect to BS congestion rate λ_C.

It is seen from the plot in Figure 7.5 that the single MNO system has a steep decrease in asymptotic availability as the BS congestion rate λ_C increases, going up to almost three congestion failures per month. The asymptotic availability of the multihomed system stays relatively high, also for an increased BS congestion rate.

This observation suggest that for areas susceptible to BS congestion, e.g. in areas with lots of infrastructure or social events, using multihomed SUs is preferable.

Chapter 8
Use Case 3: Cascading Base Station Cyber Failure

As the smart grids of the future becomes smarter, they will rely more and more on ICT and backbone networks, where it is quite possible that cyber failures could cascade between SW in BSs. There are few relevant examples of malware affecting and propagating between BSs or other MNO components per today, but the possibility of malware doing so in the future is, and should be, a legitimate concern.

It is assumed that a SW error in a BS caused by malware can propagate to other BSs in the MNO. Given that the affected ICT system of the MNO is connected somehow to other ICT systems, e.g. if the two MNOs share ICT resources of some kind, the error can cascade to the other systems, i.e. to a BS in another MNO. The more BSs that are affected, the more likely the error will propagate to other BSs, though the threshold for cascading from a BS in one MNO to a BS in the other MNO is presumably higher than for the error to propagate between BSs within the same MNO.

In the following sections BSs could be in a working state, an error state or in a failed state [ALRL04], where both BSs in the error state and in the failed state are assumed to be able to propagate SW errors to other BSs. Also, the BSs are assumed not to fail for any other reasons than failure caused by SW errors. Figure 8.1 shows the steps in which an error or failure in a BS can propagate to other BSs in an MNO and cascade to BSs in the other MNO. The steps from Figure 8.1 are gone through and explained further in the following sections.

8.1 Single BS Cyber Failure

First the SU is assumed to only be able to connect to a single BS prone to SW errors because of malware. A BS error is not the same as a BS failure, but can lead to a failure if left untreated. The rate of which a BS gets infected with malware and enters the error state is assumed to be λ_{Er}, and if a BS is in the error state, the failure rate is assumed to be λ_F. The malware infection of a single BS is seen in

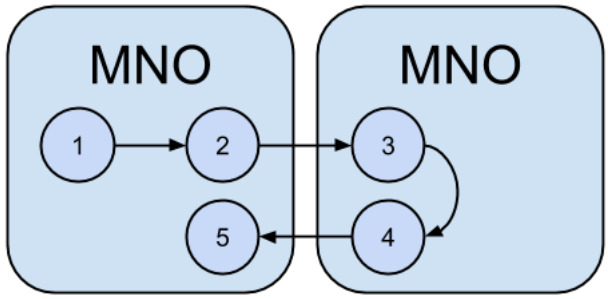

Figure 8.1: Steps of a cascading BS cyber failure; (1) malware infection of a BS in an MNO, (2) propagation of BS malware in an MNO, (3) cascading of BS malware to a second MNO, (4) propagation of BS malware in a second MNO, and (5) cascading of BS malware back to the first MNO.

Figure 8.2 as the first step, (1) malware infection of a BS in an MNO. The BSs are assumed to self-restore by reboot or remote configuration in the case of a malware error or failure, giving the BSs an independent repair rate of μ_{Er} from the error state and μ_F from the failed state. However, as SW errors can be hard to detect before they manifest as a failure, the repair rate from error state is relatively low compared to the repair rate from the failed state. With these rates known and assuming the SU can only connect to a single BS, a simple dependability model of a single BS system can be made as seen in Figure 7.2.

With the steady state probabilities from the dependability model in Figure 8.2, denoted $\underline{p} = \{p_W, p_E, p_F\}$, the probability of the BS being in the error or failed state where it can possibly propagate malware to other BSs is obtained by adding up the steady state probabilities of the error and failure states, as shown in (8.1). The asymptotic availability A_{BS} of the single BS system is obtained by adding up steady state probabilities of the working and error states, as shown in (6.2).

$$P\{\text{BS Malware}\} = P_M = p_E + p_F \tag{8.1}$$

$$A_{BS} = p_W + p_E \tag{8.2}$$

8.2 Propagating BS Cyber Failure

Assuming the SU only has one SIM card, it can only connect to BSs belonging to one of the MNOs, and the propagation of BS malware in that MNO has to be regarded when doing a availability analysis. The malware infection of a single BS is seen in

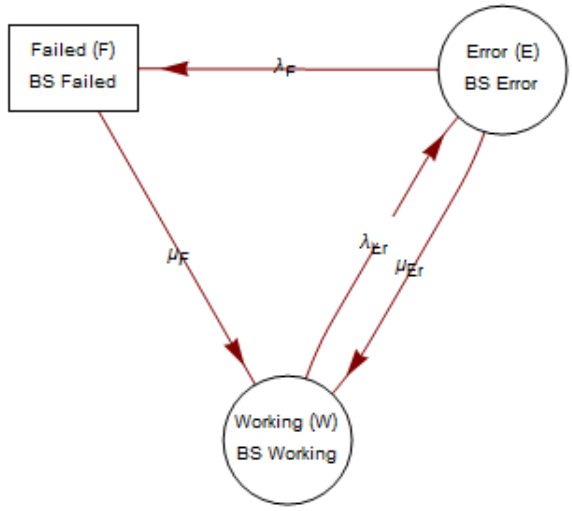

Figure 8.2: Markov dependability model of cyber error and failure in single BS.

Figure 8.1 as the first step, (1) malware infection of a BS in an MNO. When a BS gets infected it will propagation malware to remaining uninfected BSs in the MNO, seen in Figure 7.1 as the second step, (2) propagation of BS malware in an MNO.

The rate at which a BS in an MNO gets infected with malware and goes to the error state is λ_{Er}. When a BS in an MNO is infected with malware, implicitly being in either the error or the failure state, the BS increases the rate at which other BSs in the MNO gets infected malware realized with a malware constant m_{BS}, i.e. the error rate for remaining normal working BSs becomes $(1 + m_{BS})\lambda_{Er}$. Likewise, when two out of three BSs in an MNO are infected with malware the error rate for the last normal working BS becomes $(1 + 2m_{BS})\lambda_{Er}$. Still the failure rate when in BS error state is λ_F. State space of the single MNO system is defined as $\Omega = \{\{i\text{BS Error}, j\text{BS Failed}\} \mid i \in \{0,1,2,3\}, j \in \{0,1,2,3\}, i + j \leq 3\}$, giving the dependability model as seen in Figure 8.3.

With the steady state probabilities from the dependability model in Figure 8.3, denoted $\underline{p} = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{10}\}$, the asymptotic availability of the single MNO system with BS malware propagation can be obtained. The MNO system is working as long as at least one BS in that MNO is working, giving the system

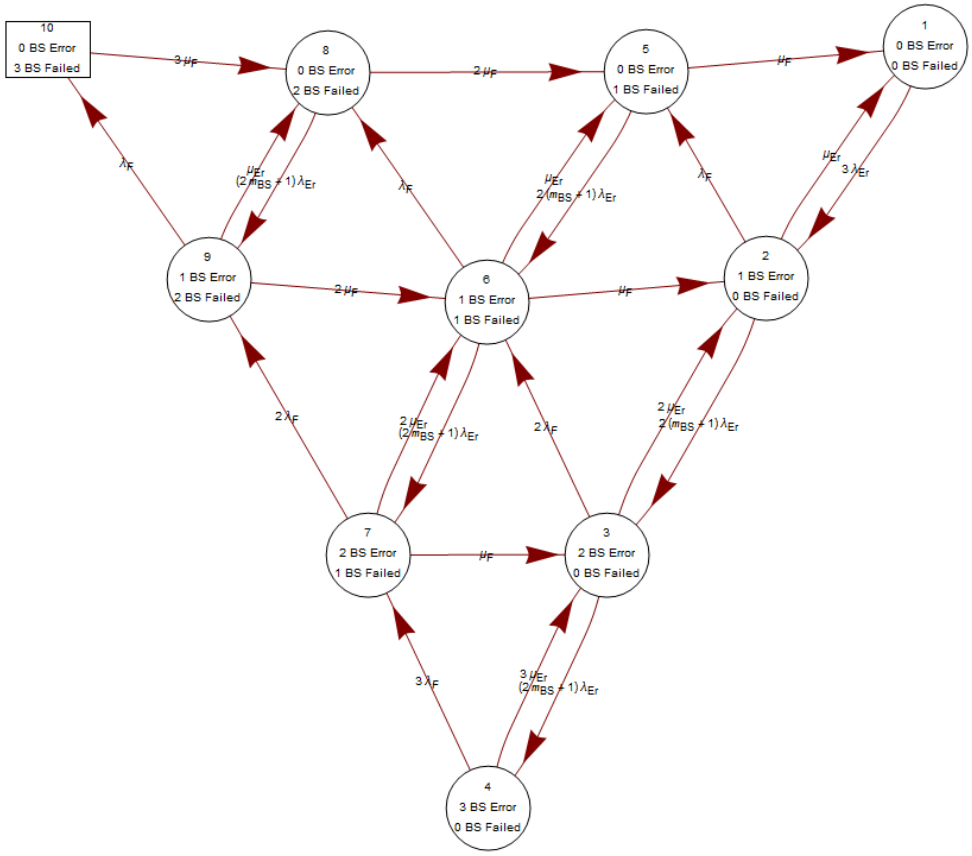

Figure 8.3: Markov dependability model of a single MNO system with malware propagation between BSs.

asymptotic availability A_{MNO} as seen in (8.3).

$$A_{MNO} = p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + p_7 + p_8 + p_9 = 0.999999 \tag{8.3}$$

8.3 Cascading BS Cyber Failure

To obtain the asymptotic availability of the whole smart grid system from Figure 4.1 both MNOs and all six BSs have to be regarded. Considering MNO could use third-party network or component providers, or use common maintenance services moving between BSs from both MNOs, malware could in this way cascade between BSs in different MNOs. Depending on what services that is shared or commonly

used by the MNOs, the rate at which malware can cascade between MNOs will vary, where in this analysis it is assumed that there is a threshold for cascading malware to the other MNO higher than that of malware propagating between BSs inside a single MNO.

8.3.1 MNO Cyber Dependency

The infection of the first BS is seen in Figure 8.1 as the first step, (1) malware infection of a BS in an MNO. When a BS is infected it will propagate malware inside the MNO, seen in Figure 8.1 as the second step, (2) propagation of BS malware in an MNO. Also, BS malware will cascade to the second MNO seen in Figure 8.1 as the third step, (3) cascading of BS malware to a second MNO. If at least one BS gets infected in the second MNO, malware will also propagate between BSs in this MNO, seen as the fourth step, (4) propagation of BS malware in a second MNO.

Assuming that for each BS infected with malware in an MNO there is an increase in the rate at which BSs in the other MNO gets malware infected with a third of the malware constant m_{BS}. The increase in BS error rate due to malware cascading from BSs in the other MNO is in addition to any error rate increase caused by malware propagation already existing in between BSs in the MNO. Thus, looking at the dependability model from Figure 8.3, BS malware cascading happen when the MNO system is any state but state 1. When an MNO is in state 2 or state 5 the error rate of the BSs in the other MNO is increased with $\frac{1}{3}m_{BS}$, when the MNO is in state 3, state 6 or state 8 the other MNO's BS error rate is increased by $\frac{2}{3}m_{BS}$, and when the MNO is in state 4, state 7, state 9 or state 10 the other MNO's BS error rate is increased by $\frac{3}{3}m_{BS} = m_{BS}$.

With the steady state probabilities from the dependability model seen in Figure 8.3 a mean error rate increase for the second MNO can be obtained. By adding all error rate increases m_{BS} multiplied with the steady state probability of the state in which they occur, a mean error rate increase M_{BS} for the second MNO is obtained, as seen in (8.4).

$$M_{BS} = (\frac{1}{3}(p_2 + p_5) + \frac{2}{3}(p_3 + p_6 + p_8) + (p_4 + p_7 + p_9 + p_{10}))m_{BS} \tag{8.4}$$

With the mean error rate increase for the second MNO obtained, a new MNO dependability model can be made with the extra error rate increase. For all error rates the constant M_{BS} is added, giving the dependability model as seen in Figure 8.4.

The smart grid system including both MNOs and BS malware cascading from one MNO to a the other dis working as long as at least one of the six BSs are

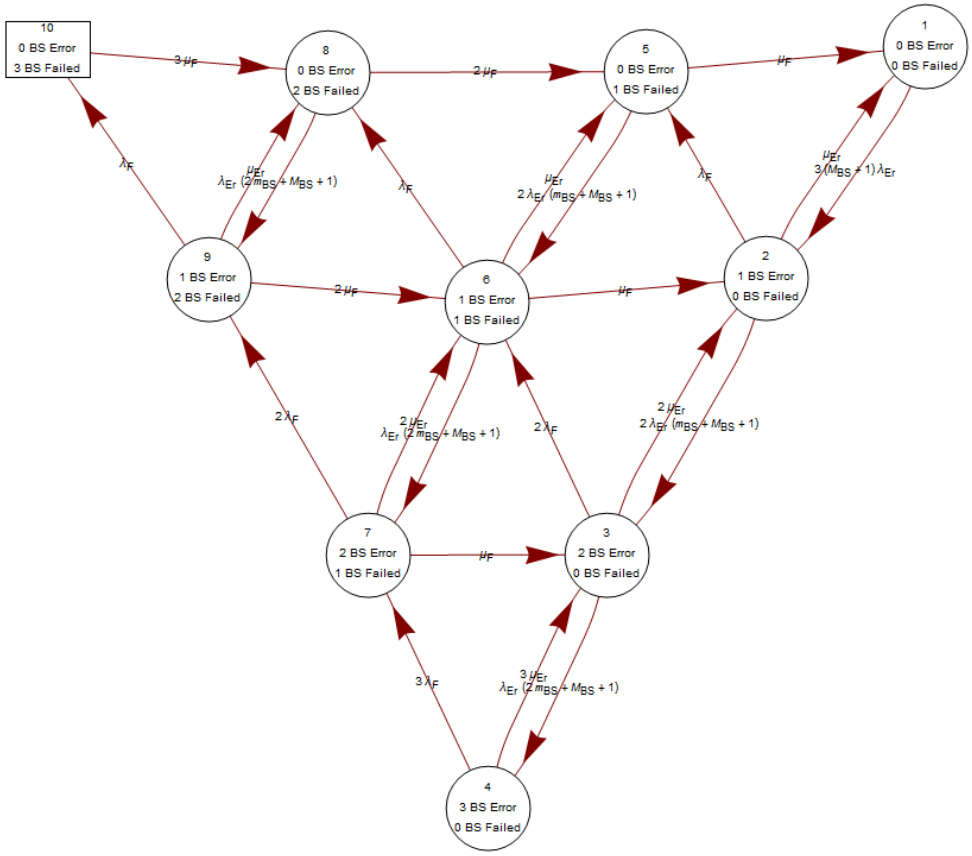

Figure 8.4: Markov dependability model of a single MNO system with malware propagation between BSs and including cascading of malware from the other MNO.

working. Using the steady state probabilities $\underline{p}$ from the system in Figure 8.3, and denoting the steady state probabilities from the system in Figure 8.4 as $\underline{p_m} = \{p_{1m}, p_{2m}, p_{3m}, p_{4m}, p_{5m}, p_{6m}, p_{7m}, p_{8m}, p_{9m}, p_{10m}\}$, the smart grid system's asymptotic availability A_{SG} can be seen in (8.6).

$$U_{SG} = P_{S10} P_{S_m 10} = 4.26 \times 10^{-13} \tag{8.5}$$

$$A_{SG} = 1 - U_{SG} \tag{8.6}$$

8.3.2 MNO Interdependency

If BS malware can cascade from one MNO to another, it will realistically cascade the other way around as well, thus creating a interdependency between the MNOs. The probability of an MNO being in a state where it can cascade malware is bigger when the MNO can experience cascaded malware from the other MNO, and thus the probability for cascading malware back gets bigger as well, enlarging the mean error rate increase M_{BS}. This interdependency with BS malware cascading back to the first MNO is seen as step five in Figure 8.1, (5) cascading of BS malware back to the first MNO.

To get a probability for BS malware cascade as precise as possible the constant M_{BS} has to be recalculated repeatedly until it converges to some value. The recalculation of M_{BS} is a manageable task with a mathematical tool, and the new numerical value for M_{BS} is seen in (8.7).

$$M_{BS} = 2.317115 \tag{8.7}$$

Using the numerically obtained error rate increase M_{BS} and the dependability model from Figure 8.4, the asymptotic availability A_{SG} for the smart grid system including MNO interdependency in the form of BS malware cascading is obtained, seen in (8.9).

$$U_{SG} = P^2_{S_m 10} = 4.71 \times 10^{-13} \tag{8.8}$$

$$A_{SG} = 1 - U_{SG} \tag{8.9}$$

8.4 Discussion

With dependability models created for the MNO systems with BS malware infection some observations are made. Like in use case 2 with BS congestion, when analysing BS malware infection the asymptotic availability of the single MNO system is remarkably lower than the asymptotic availability of the multihomed systems. What separates BS malware from congestion is that BS malware may lay dormant in BSs unnoticed, hypothetically being undetectable until causing the BS to fail. The plot in Figure 8.5 shows the asymptotic availability of the single MNO system from Figure 8.3 with $m_{BS} = 2.5$, $m_{BS} = 5$ and $m_{BS} = 10$ plotted with respect to BS error repair rate μ_{Er}.

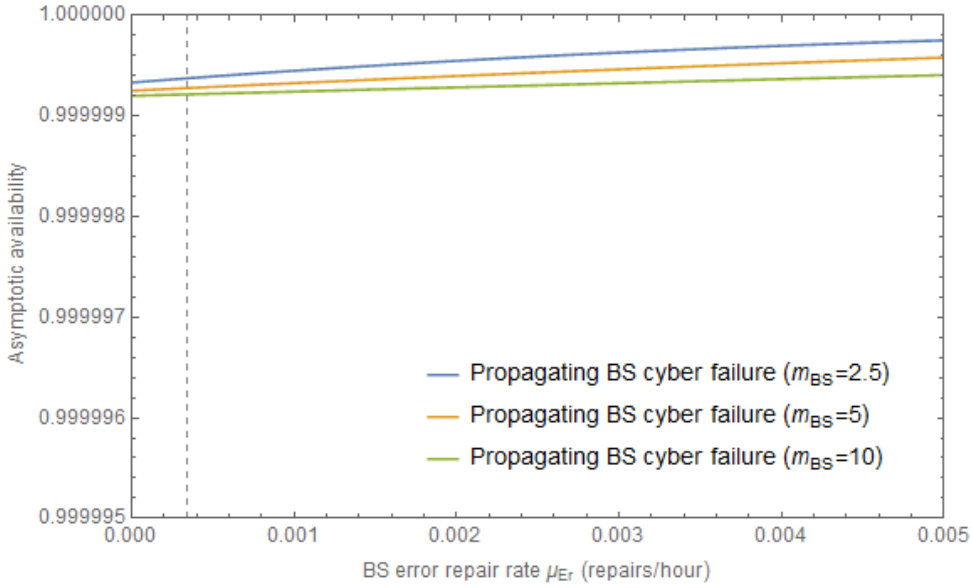

Figure 8.5: Plot of the asymptotic availability of the single MNO system from Figure 8.3 with $m_{BS} = 2.5$, $m_{BS} = 5$ and $m_{BS} = 10$ with respect to BS error repair rate μ_{Er}. The dashed grid line shows the value of the BS error repair rate μ_{Er} used in use case 2.

It is seen from the plot in Figure 8.5 that the asymptotic availability of the single MNO system stays incredibly high even when $\mu_{Er} = 0$, meaning that all errors are undetectable, and $m_{BS} = 10$, meaning that errors propagate quickly between BS in the MNO. However, malware existing in BS may not have the intention of causing BSs to fail, but rather exist to e.g. record sensitive data or intentionally lay dormant until activated [KC06]. On that note, it is interesting to look at the probability that malware infection exists in the MNO. The plot in Figure 8.6 shows the probability of that at least one of the BSs in the single MNO system from Figure 8.3 with $m_{BS} = 2.5$, $m_{BS} = 5$ and $m_{BS} = 10$ are infected with malware, plotted with respect to BS error repair rate μ_{Er}.

Even in the system with the smallest malware constant, $m_{BS} = 2.5$, and the BS error repair rate μ_{Er} being at almost one error repair per week, the probability of having malware in the MNO is still over 80%. This goes to show that in future smart grids malware could accumulate and propagate, and that one should have procedures to avoid malware infection, e.g. by having up-to-date firewalls, and have procedures to detect and remove malware in BSs.

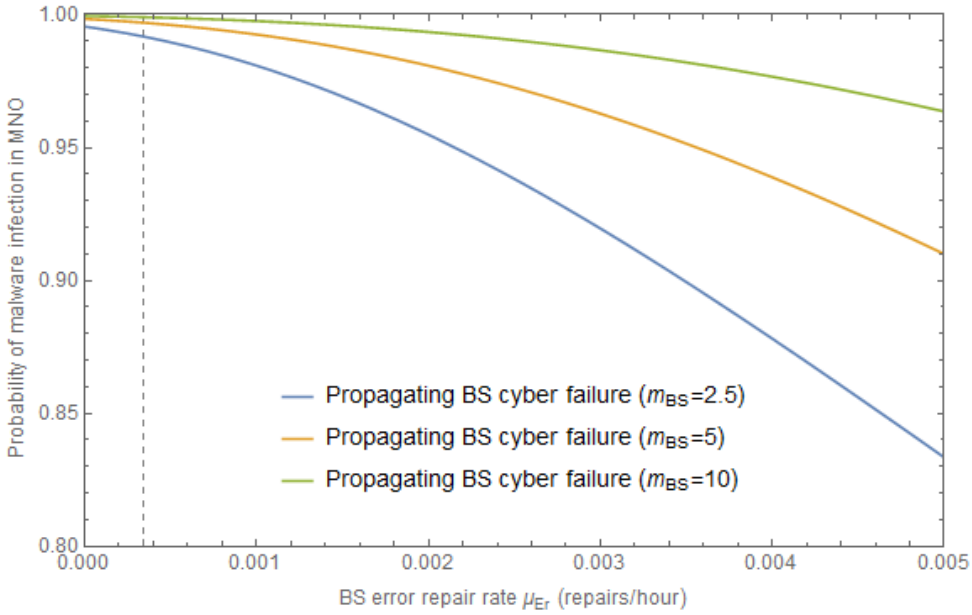

Figure 8.6: Plot of the probability of that at least one of the BSs in the single MNO system from Figure 8.3 with $m_{BS} = 2.5$, $m_{BS} = 5$ and $m_{BS} = 10$ are infected with malware with respect to BS error repair rate μ_{Er}. The dashed grid line shows the value of the BS error repair rate μ_{Er} used in use case 2.

Chapter 9
Use Case 4: Escalating Cascading Power Grid Failure

Realistically, a power grid will have some sort of power grid control system monitoring and controlling the power grid. With a failed control system the repair personnel may not be notified about a power grid failure in an adequate short amount of time, or they will have to use additional time on locating the failure, which in either situation causes longer repair time. Also, if the potentially failed control system handles critical events in the power grid improperly, e.g. if data from the power grid is incorrect when received or if the control system is treating the data wrong, the control system could handle critical events in the power grid in a non-optimal way, leading to bigger damages than if the control system had worked. With more severe damages to any failed components in the power grid, the longer it takes to repair them.

In Chapter 6 the power grid was assumed to not be dependent on any control system, while in this chapter an additional dimension is added; the states of the power grid control system. Simply put, there are four different states in which the power grid and control system could coexist, with both the power grid and the control system being in either a working or failed state, as seen in Figure 9.1.

Different factors affect the failure and repair rates of the DGs and how fast failures could cascade to the MNOs, where MNO failures contrarily can affect the state of the power grid. For reference, Figure 6.1 in Chapter 6 illustrates the chronological steps of how a failure may cascade and have effect on the power grid and the MNO systems in the smart grid from Figure 4.1. The steps from Figure 6.1 are gone through and explained in the sections in Chapter 6, where this use case follows the same chronological steps and will therefore not explain the steps further in the following sections.

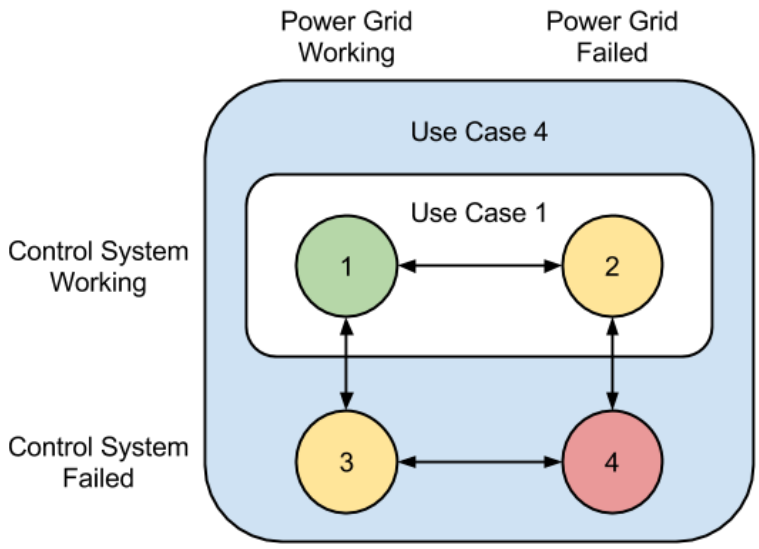

Figure 9.1: Comparison of dimensions analysed in Use Case 1 and Use Case 4. In state 1 both the power grid and control system are working, in state 2 the power grid has failed while the control system is working, in state 4 the power grid is working while the control system has failed, and in state 4 both the power grid and control system has failed.

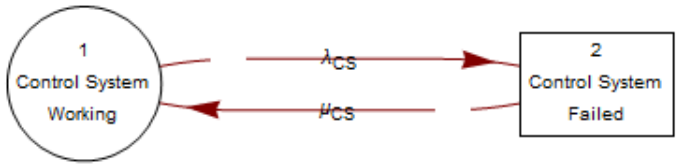

Figure 9.2: Markov dependability model of the power grid control system.

9.1 Control System Failure

The power grid control system can be regarded as either working or failed, and having a failure rate λ_{CS} and a repair rate μ_{CS}. The state space of the model is then defined as $\Omega = \{$Control System Working, Control System Failed$\}$, giving rise to a simple Markov dependability model as seen in Figure 9.2.

The power grid control system has only two states, working and failed, letting the availability, i.e. probability that the power grid control system is working, be

obtained as seen in (9.1) [KB09].

$$A_{CS} = P_{CS} = \frac{\lambda_{CS}^{-1}}{\mu_{CS}^{-1} + \lambda_{CS}^{-1}} \tag{9.1}$$

9.2 Escalated Cascading Power Grid Failure

In this section the BSs are assumed to be without any power backup and they do not fail due to any other reasons than lack of power. A failure of DG A or DG B will immediately cascade to the BSs in MNO A or MNO B respectively, causing them to fail.

The power grid control system is assumed to work such that when the control system is working the smart grid system behaves as in Use Case 1 in Chapter 6, while if the control system is in failed state the repair times of DG A and DG B are increased. The increase in repair time is realized with a managing constant m_{CS}, where if the control system has failed the repair rates μ_{DG} of the DGs are reduced with m_{CS} and becomes $(1 - m_{CS})\mu_{DG}$.

9.2.1 Single Distribution Grid Dependency

First looking at a system where the SU is not multihomed and can only connect to BSs belonging to one MNO. In this dependability model only one of the DGs has to be regarded, the DG powering the one active MNO, with two possible scenarios for DG repair, one where the control system is working and one where it is not.

Knowing the failure and repair rates of both the control system and the DG, a dependability model of the DG system can be modeled. State space of the DG system is defined as $\Omega = \{\{i\text{DG Working}, j\text{CS Working}\} \mid i, j \in \{0, 1\}\}$, and the system is defined as working when the DG is working, giving the dependability model as seen in Figure 9.3.

With the steady state probabilities from the dependability model in Figure 9.3, denoted $\underline{p} = \{p_1, p_2, p_3, p_4\}$, the asymptotic availability A_{DG} of the DG system including the power grid control system can be obtained by adding the steady state probabilities of the working states, as seen in (9.2).

$$A_S = p_1 + p_3 = 0.998625 \tag{9.2}$$

With the asymptotic availability, or working probability P_{CS}, for the power grid control system, the dependability model seen in Figure 9.3 can be made simpler and

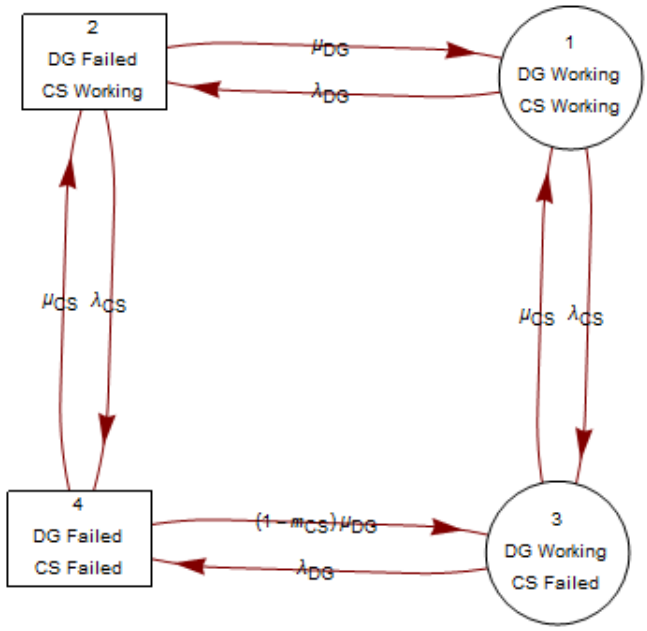

Figure 9.3: Markov dependability model of a single DG system including a power grid control system.

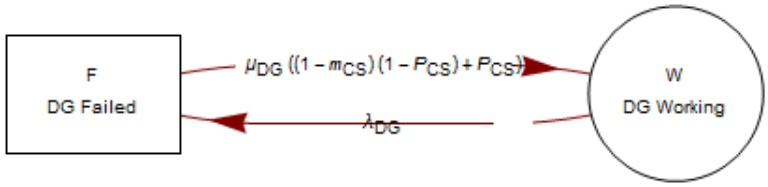

Figure 9.4: Markov dependability model of a single DG system including a power grid control system.

modelled as a simple two-state Markov chain. The DG has a repair rate μ_{DG} for when the control system is working with probability P_{CS} and a repair rate $(1 - m_{CS})\mu_{DG}$ for when the control system is failed with probability $(1 - P_{CS})$, thus giving the DG a total repair rate of $(P_{CS} + (1 - P_{CS})(1 - m_{CS}))\mu_{DG}$. State space of the DG system is then defined as $\Omega = \{\{i\text{DG Working}\} \mid i \in \{0, 1\}\}$, giving the dependability model as seen in Figure 9.4.

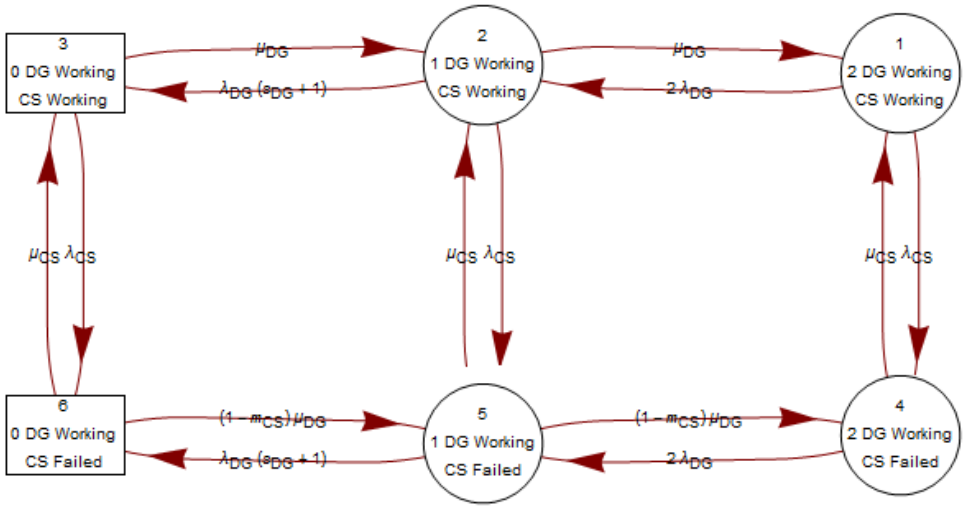

Figure 9.5: Markov dependability model of the smart grid including a power grid control system.

9.2.2 Power Grid Dependency

With multihoming the SU in the smart grid system can connect to both MNOs, and both DGs have to be regarded in the dependability model of the smart grid system. With both DGs regarded the propagation of stress between them will also have to be regarded, realized with a DG stress constant s_{DG} as in Use Case 1 in Chapter 6. The state space of the power grid system including the control system is defined as $\Omega = \{\{i\text{DG Working}, j\text{CS Working}\} \mid i \in \{0,1,2\}, j \in \{0,1\}\}$. Knowing the failure rate λ_{DG} and repair rate μ_{DG} of the DGs, the failure rate λ_{CS} and repair rate μ_{CS} of the control system, and including the stress propagation between the DGs, the dependability model becomes as seen in Figure 9.5.

With the steady state probabilities from the dependability model in Figure 9.5, denoted $\underline{p} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, the asymptotic availability A_{SG} of the smart grid system including the power grid control system is obtained by adding the steady state probabilities of the working states, as seen in (9.3).

$$A_{SG} = p_1 + p_2 + p_4 + p_5 = 0.999991 \tag{9.3}$$

With the working probability P_{CS} for the power grid control system, the dependability model seen in Figure 9.5 can be made simpler and modelled as a simple three-state Markov chain. The DGs have a repair rate μ_{DG} for when the control

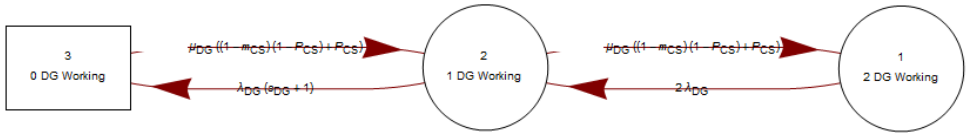

Figure 9.6: Markov dependability model of the smart grid including a power grid control system and stress propagation between DGs.

system is working with probability P_{CS} and a repair rate $(1 - m_{CS})\mu_{DG}$ for when the control system is failed with probability $(1 - P_{CS})$, thus giving the DG a total repair rate of $(P_{CS} + (1 - P_{CS})(1 - m_{CS}))\mu_{DG}$. State space of the power grid system is then defined as $\Omega = \{\{i\text{DG Working}\} \mid i \in \{0, 1, 2\}\}$, giving the dependability model as seen in Figure 9.6.

9.2.3 Power Grid & MNO Interdependency

Including the repair crew telecommunication dependency to the smart grid system introduces potentially increased repair time, as already looked at in Section 6.1.3 and Section 6.2.4. Decreasing the repair rate μ_{DG} of the DGs with a communication constant c_{DG} when all BSs have failed gives a more realistic dependability model, having a smaller asymptotic availability than a model not including the repair crew telecommunication dependency. Defining the state space as $\Omega = \{\{i\text{DG Working}, j\text{CS Working}\} \mid i \in \{0, 1, 2\}, j \in \{0, 1\}\}$, the model becomes as seen in Figure 9.7.

With the steady state probabilities from the dependability model in Figure 9.7, denoted $\underline{p} = \{p_1, p_2, p_3, p_4, p_5, p_6\}$, the asymptotic availability A_{SG} of the smart grid system including a power grid control system, stress propagation between DGs and repair crew telecommunication dependency is obtained by adding the steady state probabilities of the working states, as seen in (9.4).

$$A_{SG} = p_1 + p_2 = 0.999981 \tag{9.4}$$

Again, with the working probability P_{CS} for the power grid control system, the dependability model seen in Figure 9.5 can be made simpler and modelled as a simple three-state Markov chain. The DGs have a repair rate μ_{DG} for when the control system is working with probability P_{CS} and a repair rate $(1 - m_{CS})\mu_{DG}$ for when the control system is failed with probability $(1 - P_{CS})$, thus giving the DG a total repair rate of $(P_{CS} + (1 - P_{CS})(1 - m_{CS}))\mu_{DG}$ if at least one DG is still working.

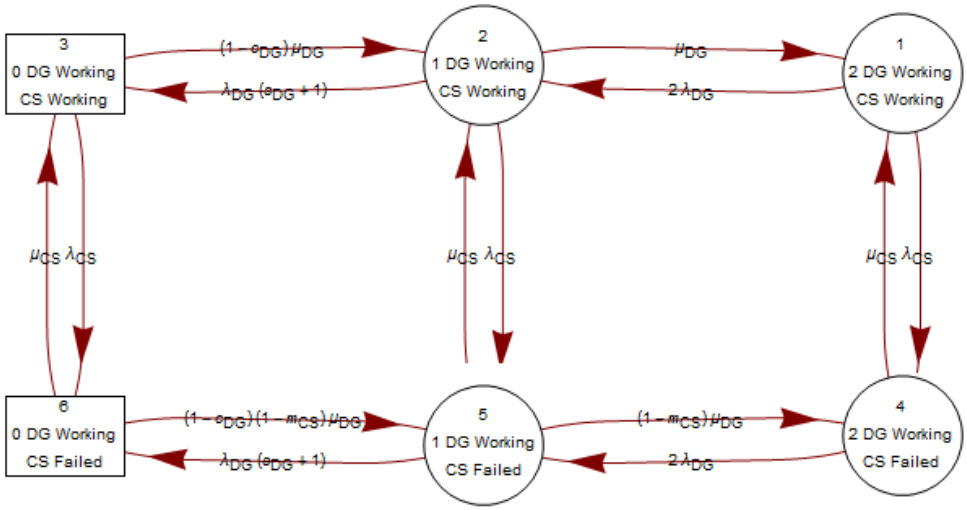

Figure 9.7: Markov dependability model of the smart grid including a power grid control system, stress propagation between DGs and repair crew telecommunication dependency.

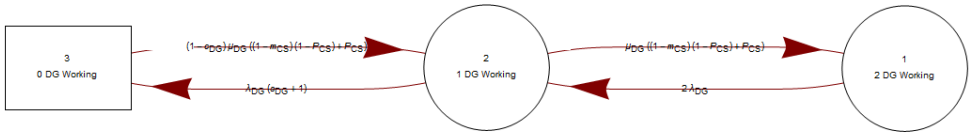

Figure 9.8: Markov dependability model of the smart grid including a power grid control system, stress propagation between DGs and repair crew telecommunication dependency.

If both DGs have failed the repair rate is also decreased with the communication constant c_{DG} and becomes $(P_{CS} + (1 - P_{CS})(1 - m_{CS}))(1 - c_{DG})\mu_{DG}$. State space of the power grid system is then defined as $\Omega = \{\{i\text{DG Working}\} \mid i \in \{0, 1, 2\}\}$, giving the dependability model as seen in Figure 9.8.

9.3 Escalated Cascading Power Grid Failure with BS Power Backup

BSs in a real system will often have power backup of some kind, e.g. diesel generators or batteries [Mal10]. When introducing power backup for the BSs there will be an

extra delay between the moment a DG fails and the moment its dependent BSs fails, which means that the smart grid system asymptotic availabilities obtained from (9.3) and (9.4) are too low if the BSs have power backup.

When BS power backup is included in the dependability models an extra state space dimension is formed. Because the complexity of Markov dependability models grows exponentially when adding dimensions to the state space, a state space with fewer dimensions is preferable. Since the power grid control system is assumed to be independent from the power grid and BSs, the control system can be represented in the dependability models with the control system's working probability P_{CS}, as already seen from the dependability models in Figure 9.6 and Figure 9.8. The dependability models of the smart grid system including BS power backup will all use the probability P_{CS} instead of the power grid control system dimension.

9.3.1 Single Distribution Grid Dependency

Assuming that the SU has only one SIM card and can only connect to BSs belonging to one MNO, only one of the DGs has to be regarded, the one powering the applicable MNO. The state space for this single MNO system is defined as $\Omega = \{\{i\text{TL Working}, j\text{BS Working}\} \mid i \in \{0,1\}, j \in \{0,1,2,3\}, j \geq 3i\}\}$, including the state of the one DG and the BSs. In this single MNO system, if the DG, all three BSs has to run out of power before the MNO system fails, each BS with power run out rate λ_{PB}. Knowing the failure rate λ_{DG} and the repair rate μ_{DG} of the DGs, assuming that DG failures happen rarely enough for the BSs power backup to recharge between DG failures, and including the repair crew telecommunication dependency using the control system's working probability P_{CS}, the dependability model becomes as seen in Figure 9.9.

With the steady state probabilities from the dependability model, denoted $\underline{p} = \{p_1, p_2, p_3, p_4, p_5\}$, the asymptotic availability A_{MNO} of the MNO system is obtained by adding up the steady state probabilities of the working states from, as shown in (9.5).

$$A_{MNO} = p_1 + p_2 + p_3 + p_4 = 0.999756 \tag{9.5}$$

9.3.2 Power Grid Dependency

Assuming the SU is multihomed and can connect to both MNOs, when a DGs fails the failure rate of the other DG is increased with a stress constant s_{DG}. This means that if a DG has failed the potentially remaining working DG would have an increased DG failure rate; more specifically the DG failure rate becomes $(1 + s_{DG})\lambda_{DG}$. Also, the DGs have an increased repair time if the power grid control system is failed,

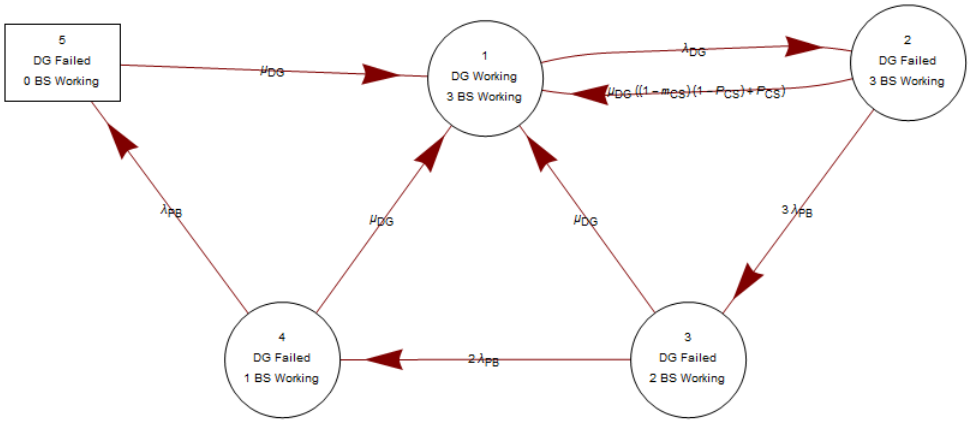

Figure 9.9: Markov dependability model of a single MNO system including BS power backup and a power grid control system.

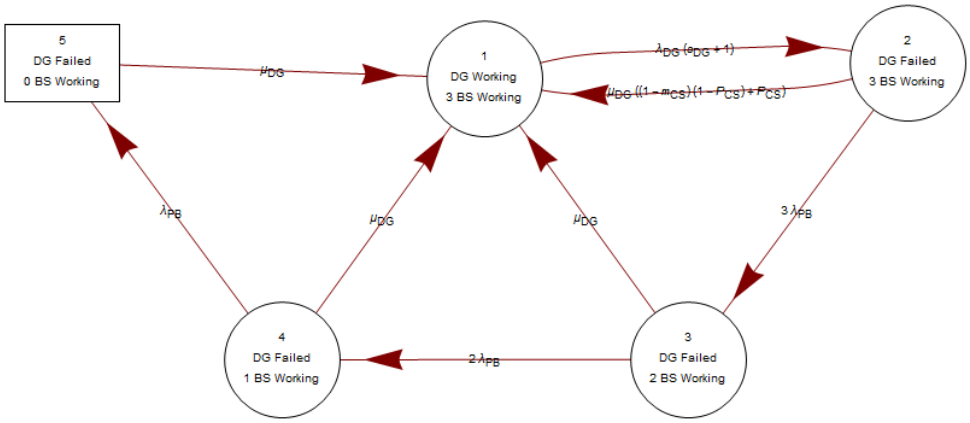

Figure 9.10: Markov dependability model of a single MNO system including BS power backup and a power grid control system with increased DG stress.

realized with the managing constant m_{CS}. The dependability model of a DG and all three dependent BSs in the case of increased DG stress is seen in Figure 9.10.

The dependability models from Figure 9.9 and Figure 9.10 can be used to make a new model for calculating the smart grid system asymptotic availability. Denoting the steady state probabilities from the dependability model in Figure 9.10 as $\underline{p_s} = \{p_{1s}, p_{2s}, p_{3s}, p_{4s}, p_{5s}\}$, and using the already denoted steady state probabilities $\underline{p}$ from the dependability model in Figure 9.9, the failure rate λ_{MNO} of the system

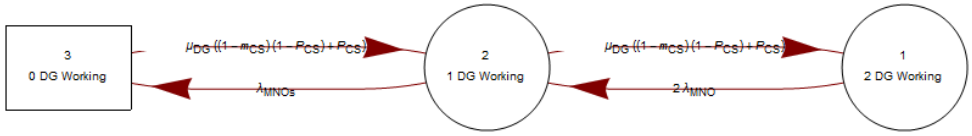

Figure 9.11: Markov dependability model of the smart grid system from Figure 4.1 including stress propagation between DGs, BS power backup, a power grid control system and repair crew telecommunication dependency.

in Figure 9.9 and the failure rate λ_{MNOs} of the system in Figure 9.10 are obtained in (9.6) and (9.7) respectively.

$$\lambda_{MNO} = \frac{p_4}{p_1 + p_2 + p_3 + p_4}\lambda_{PB} \tag{9.6}$$

$$\lambda_{MNOs} = \frac{p_{4s}}{p_{1s} + p_{2s} + p_{3s} + p_{4s}}\lambda_{PB} \tag{9.7}$$

A dependability model of the smart grid system is made with state space defined as $\Omega = \{i\text{MNO Working}\} \mid i \in \{0, 2\}\}$, including both the DGs and the BSs with power backup. With the failure rates λ_{MNO} and λ_{MNOs} obtained and knowing the repair rate μ_{DG} of the DGs and the control system's working probability P_{CS}, the dependability model becomes as seen in Figure 9.11.

With the steady state probabilities from the dependability model in Figure 9.11, denoted $\underline{p_{SG}} = \{p_{1sg}, p_{2sg}, p_{3sg}\}$, the asymptotic availability A_{SG} of the smart grid system including stress propagation between DGs, BS power backup and the repair crew telecommunication dependency is obtained by adding up the e steady state probabilities of the working states, as shown in (9.9).

$$U_{SG} = p_{3sg} = 2.98 \times 10^{-7} \tag{9.8}$$

$$A_{SG} = p_{1sg} + p_{2sg} = 1 - U_{SG} \tag{9.9}$$

9.3.3 Power Grid & MNO Interdependency

Including the repair crew interdependency, the repair time for the DGs when all BSs have failed will be somewhat increased. With the obtained failure rates for the MNO

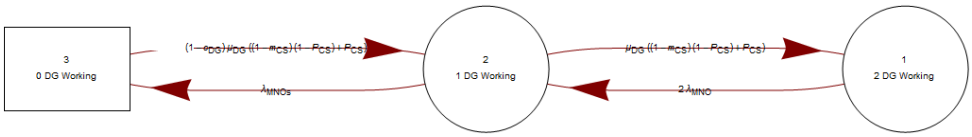

Figure 9.12: Model of the smart grid system from Figure 4.1 including redirection of load when transmission line failures occur, MNO dependency, BS power backup and the power grid control system.

systems λ_{MNO} and λ_{MNOs}, a new dependability model of the smart grid system including the repair crew interdependency is easily obtained.

For the new model of the smart grid the only rate changing from the model in Figure 9.11 is the repair rate from the failed state, which will be decreased by the communication constant c_{DG}. The state space of this new model is defined as $\Omega = \{i\text{MNO Working}\} \mid i \in \{0, 2\}\}$, giving the model as seen in Figure 9.12.

With the steady state probabilities from the dependability model in Figure 9.12, denoted $p_{SG} = \{p_{1sg}, p_{2sg}, p_{3sg}\}$, the asymptotic availability A_{SG} of the smart grid system including stress propagation between DGs, repair crew telecommunication dependency, the control system's working probability P_{CS} and BS power backup is obtained by adding up the steady state probabilities of the working states, as shown in (9.10).

$$A_S = p_{S1} + p_{S2} = 0.999999 \tag{9.10}$$

9.4 Discussion

With the dependability models created for the smart grid systems with or without multihoming, repair crew telecommunication dependency and BS power backup, a comparison of the systems with regard to asymptotic availability can be made. In the discussion from Chapter 6 the smart grid systems was plotted with respect to DG failure rate λ_{DG}, BS power backup run out rate λ_{PB} and the communication constant c_{DG}, while in this use case an additional factor is added to the systems, the power grid control system. Plotting the systems from this use case with respect to λ_{DG}, λ_{PB} or c_{DG} would reveal little new insight besides what is seen in Chapter 6, analysing the effects of the power grid control system's asymptotic availability is of more interest.

The plot in Figure 9.13 shows the asymptotic availability of the single DG system

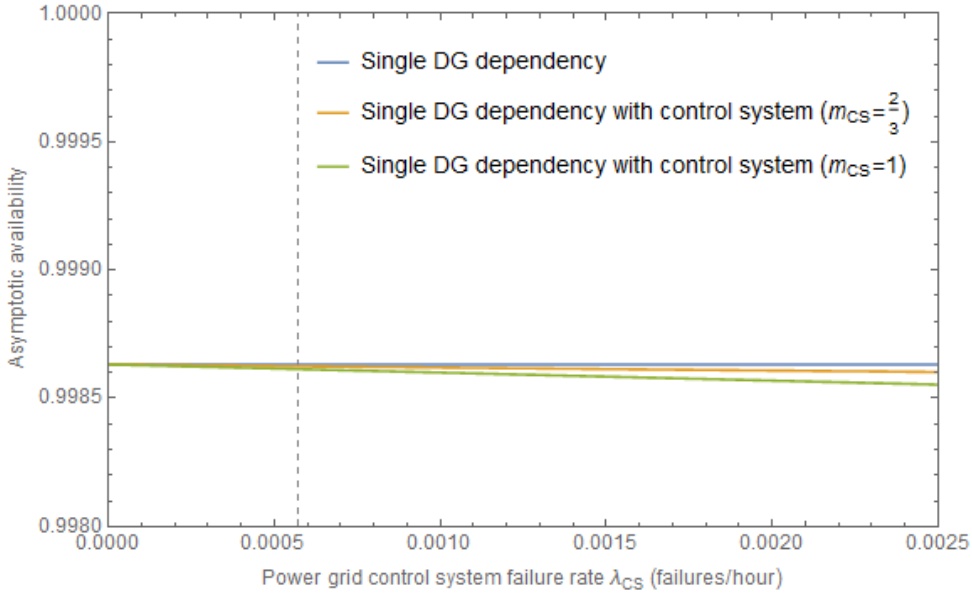

Figure 9.13: Plot of the asymptotic availability of the single DG systems from Figure 6.2, Figure 9.3 with $m_{CS} = \frac{2}{3}$ and Figure 9.3 with $m_{CS} = 1$ with respect to power grid control system failure rate λ_{CS}. The dashed grid line shows the value of the failure rate λ_{CS} used in use case 4.

from Chapter 6 and the single DG system from this use case, shown in Figure 6.2 and Figure 9.3 respectively, plotted with respect to the power grid control system failure rate λ_{CS}. In addition there is a third system, the same as the system from Figure 9.3 but with $m_{CS} = 1$, meaning that the repair rate of the system's DG is zero as long as the power grid control system is failed.

It is seen from the plot in Figure 9.13 that the asymptotic availability of the single DG systems takes little effect from a higher power grid control system failure rate λ_{CS}, even with $m_{CS} = 1$ and λ_{CS} increasing to almost two failures per month. Based on the observation from the plot in Figure 9.13, the control system's effect on the multihomed smart grid systems asymptotic availability is presumably very small. Because of this, rather than looking at the multihomed smart grid systems' asymptotic availability with respect to λ_{CS}, they are plotted with respect to the control system's asymptotic availability A_{CS}. The smart grid systems' asymptotic availability plotted are the ones from the multihomed systems with telecommunication repair crew dependency, with and without BS power backup, $m_{CS} = \frac{2}{3}$ and $m_{CS} = 1$, as seen in Figure 9.14.

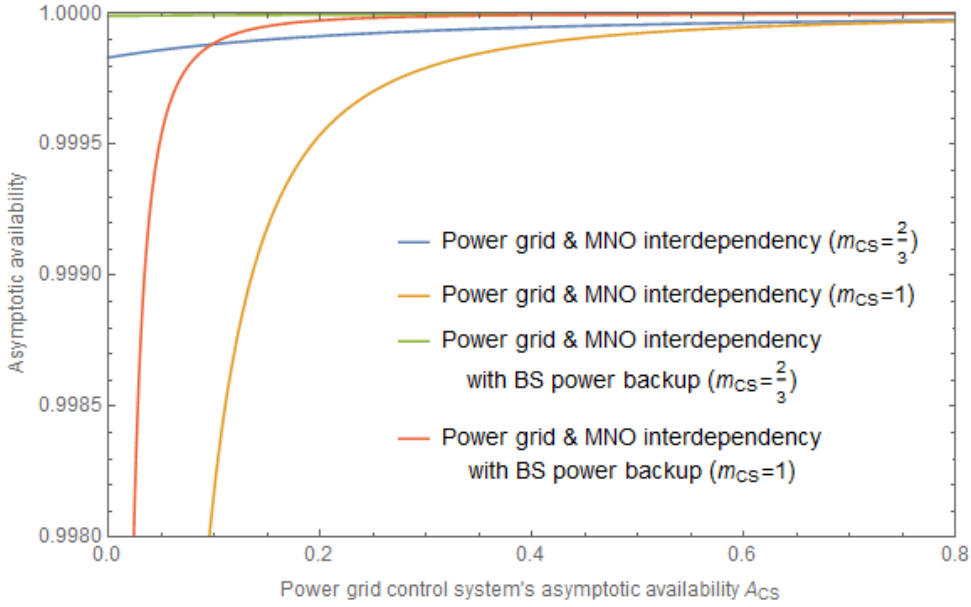

Figure 9.14: Plot of the asymptotic availability of the smart grid systems from Figure 9.7 with $m_{CS} = \frac{2}{3}$, Figure 9.7 with $m_{CS} = 1$, Figure 9.12 with $m_{CS} = \frac{2}{3}$ and Figure 9.12 with $m_{CS} = 1$ with respect to the power grid control system's asymptotic availability A_{CS}.

Naturally, for the two systems where $m_{CS} = 1$, the asymptotic availability decreases drastically when the asymptotic availability of the power grid control system approaches zero. Still, the multihomed system with BS power backup and $m_{CS} = 1$ keep a high asymptotic availability longer than the corresponding system without BS power backup, indicating that in a critical situation where the power grid control system operates on an asymptotic availability of about 0.15 or less (not being zero), having a BS power backup makes a big difference. Also, it's worth noting that he asymptotic availability of the system with BS power backup and $m_{CS} = 1$ catch up with the asymptotic availability of the system without BS power backup and $m_{CS} = \frac{2}{3}$ on a low value of A_{CS}, clarifying the benefit of BS power backup.

Chapter 10
Use Case 5: Common Cause BS Failure with Individual Repair

Erosion of BSs due to weathering will eventually cause them to break down if the BSs are not continuously and properly maintained. In addition, a natural disaster like a hurricane, earthquake or tsunami could potentially knock out several BSs at the same time if they share a common geographical area. In Norway the most realistic natural events for causing common BS failure are drastic weather events like hurricanes, blizzards and thunderstorms.

10.1 Common Cause MNO Failure

Assuming the SU is not multihomed and can solely connect to one of the MNOs, only three BSs have to be regarded. The BSs in the MNO are assumed to be located in such a way that a storm has an equal chance of knocking out one, two or all three of the BSs, where each BS has to be repaired individually by a repair crew. There is only one repair crew belonging to the MNO which can only repair one BS at a time. Also, besides common cause BS failures, the BSs will fail individually because of normal weathering.

First looking at a dependability model not including storms causing common cause BS failure, but only normal weathering, the state space is defined as $\Omega = \{\{i\text{BS Working}\} \mid i \in \{0, 1, 2, 3\}\}$. Knowing the failure rate of BSs due to weathering λ_W and the BS repair rate μ_{BS}, the dependability model becomes as seen in Figure 10.1.

Looking at a dependability model not including normal weathering, but only storms causing common cause BS failure, the state space is still defined as $\Omega = \{\{i\text{BS Working}\} \mid i \in \{0, 1, 2, 3\}\}$. The rate of BS damaging storms is λ_S, and the BSs are assumed to be located in such a way that a storm has an equal chance of damaging one, two or three BSs with a probability $P_S = \frac{1}{6}$. The MNO system is defined as working when at least one BS is working, and the storms are assumed to

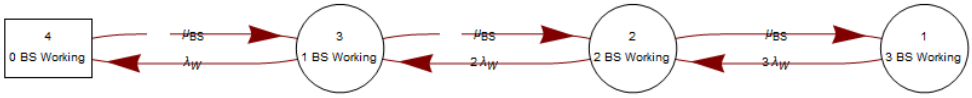

Figure 10.1: Markov dependability model of a single MNO system with BS failures caused by normal weathering.

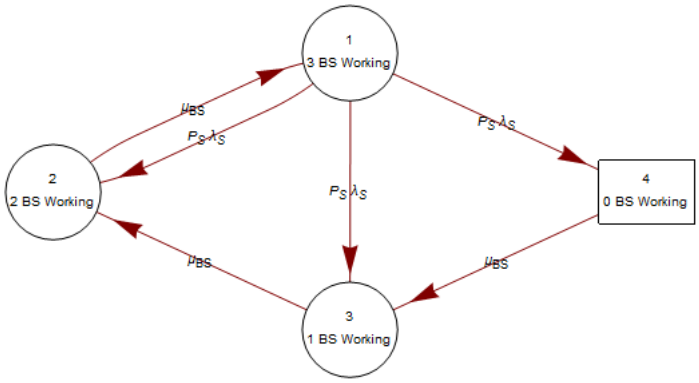

Figure 10.2: Markov dependability model of a single MNO system with common cause BS failures caused by storms.

happen rarely enough for all BSs to be repaired between storms, giving the model as seen in Figure 10.2.

By combining the two dependability models from Figure 10.1 and Figure 10.2 a final MNO dependability model is made including both BS failures caused by normal weathering and common cause BS failures caused by storms. The state space is still defined as $\Omega = \{\{i\text{BS Working}\} \mid i \in \{0, 1, 2, 3\}\}$, giving the dependability model seen in Figure 10.3.

With the steady state probabilities from the dependability model in Figure 10.3, denoted $\underline{p} = \{p_1, p_2, p_3, p_4\}$, the asymptotic availability A_{MNO} of the single MNO system with BS failures caused by weathering and storms is obtained by adding up the steady state probabilities of the working states, as seen in (10.1).

$$A_{MNO} = p_1 + p_2 + p_3 = 0.999432 \tag{10.1}$$

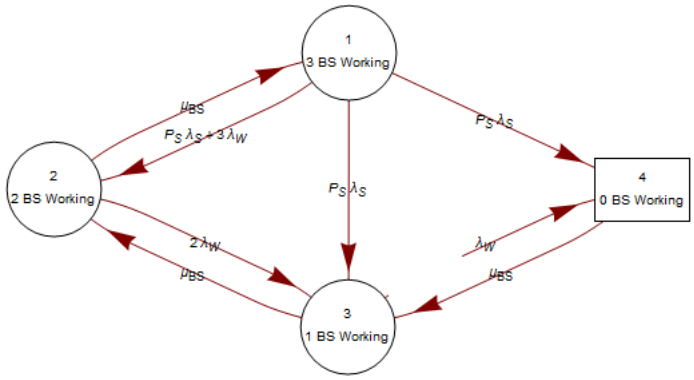

Figure 10.3: Markov dependability model of a single MNO system with BS failures caused by normal weathering and common cause BS failures caused by storms.

10.2 Common Cause Smart Grid Failure

Assuming the SU is multihomed and can connect to both MNOs, all six BSs have to be regarded when modeling. The BSs in the MNOs are assumed to be located in such a way that a storm has an equal chance of knocking out one, two three, four, five or six BSs with a probability $P_S = \frac{1}{6}$, where each BS has to be repaired individually by a repair crew, with one repair crew for each MNO. The BSs in MNO A are in this section referred to as BSA, while the BSs in MNO B are referred to as BSB.

First looking at a dependability model not including storms causing common cause BS failure, but only normal weathering, the state space is defined as $\Omega = \{\{i\text{BSA Working}, j\text{BSB Working}\} \mid i \in \{0,\ldots,3\}, j \in \{0,\ldots,3\}\}$. Knowing the failure rate of BSs due to weathering λ_W and the repair rate μ_{BS}, the dependability model becomes as seen in Figure 10.4.

Looking at a dependability model not including normal weathering, but only storms causing common cause BS failure, the state space is still defined as $\Omega = \{\{i\text{BSA Working}, j\text{BSB Working}\} \mid i \in \{0,\ldots,3\}, j \in \{0,\ldots,3\}\}$. The rate of BS damaging storms is λ_S, and the MNO system is defined as working when at least one BS is working. The storms are assumed to happen rarely enough for all BSs to be repaired between storms, with one repair crew for each MNO, giving the model as seen in Figure 10.5.

Including BS failures caused by both normal weathering and storms causing common cause BS failure into the dependability model, the state space is again defined as $\Omega = \{\{i\text{BSA Working}, j\text{BSB Working}\} \mid i \in \{0,\ldots,3\}, j \in \{0,\ldots,3\}\}$. Knowing the rate of BS damaging storms λ_S, the rate of BS failure due to normal

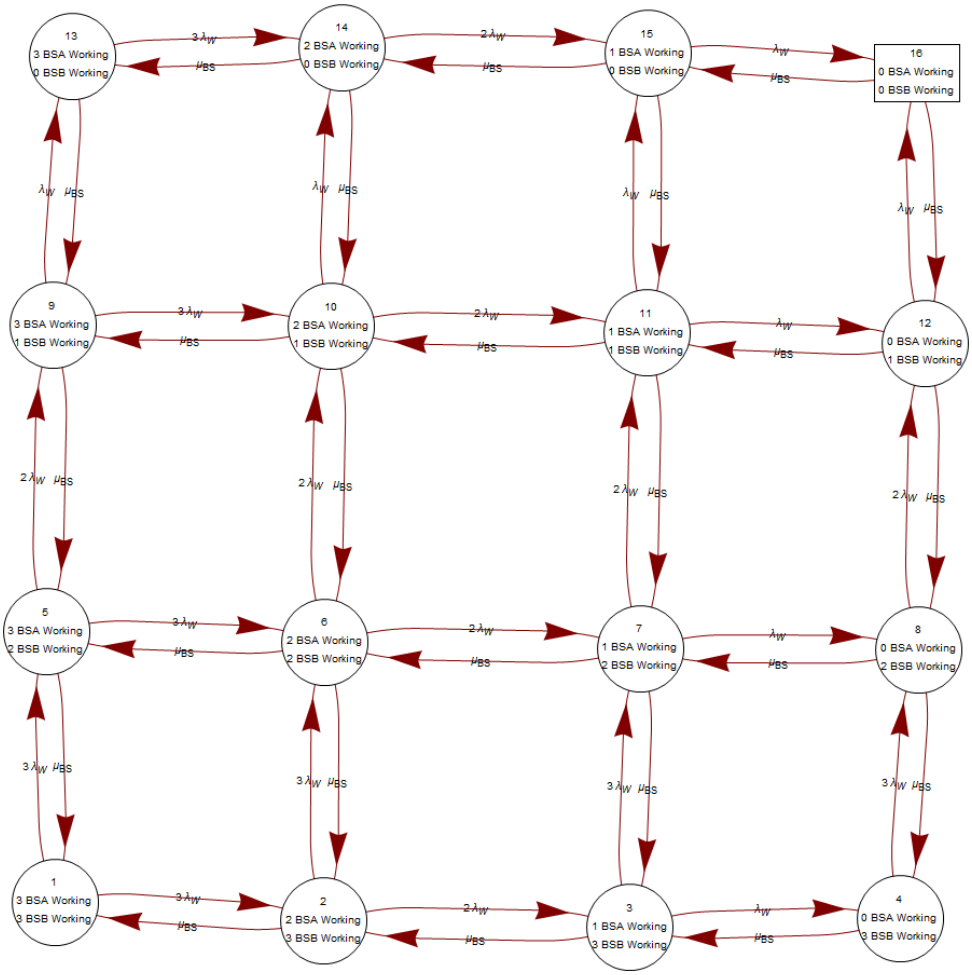

Figure 10.4: Markov dependability model of the smart grid from Figure 4.1 with BS failures caused by normal weathering.

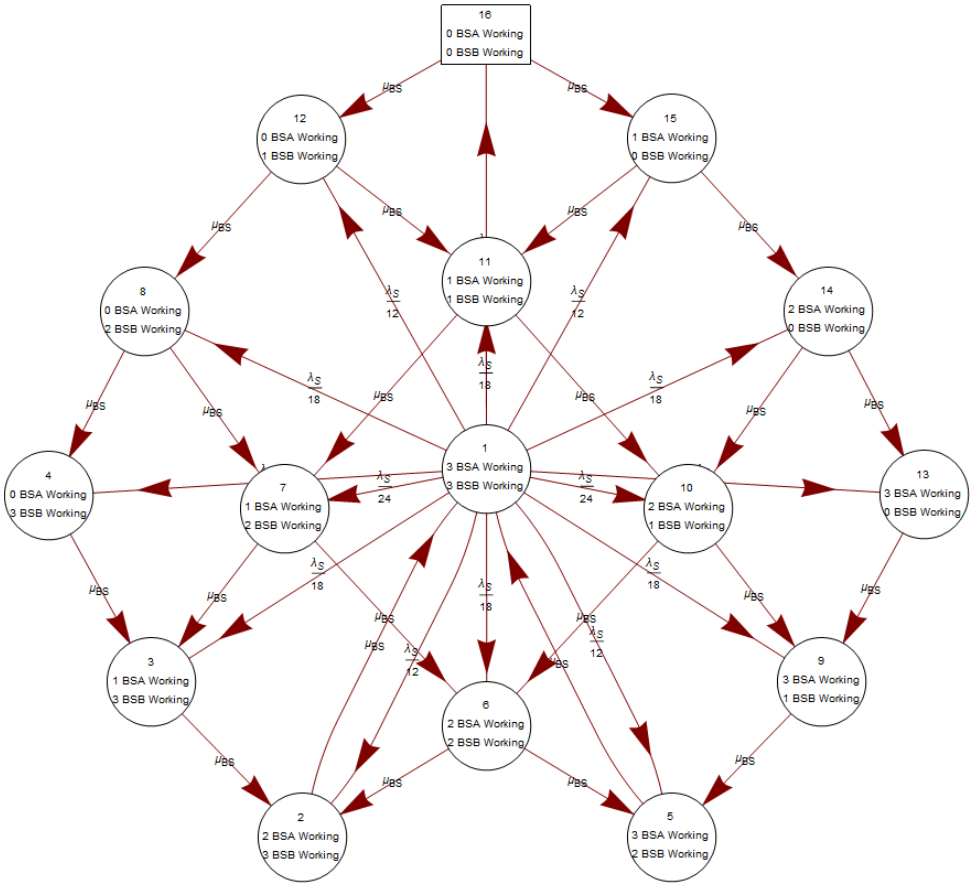

Figure 10.5: Markov dependability model of the smart grid from Figure 4.1 with common cause BS failures caused by storms.

weathering λ_W, and the repair rate of damaged BSs μ_{BS}, defined the smart grid as working when at least one BS is working, and assuming the storms are happening rarely enough for all BSs to be repaired between storms, the dependability model becomes as seen in Figure 10.6.

With the steady state probabilities from the dependability model in Figure 10.6, denoted $\underline{p} = \{p_1, \ldots, p_{16}\}$, the asymptotic availability A_{SG} of the smart grid system with BS failures caused by normal weathering and common cause BS failures caused by storms is obtained by adding up the steady state probabilities of the working states, as seen in (10.2).

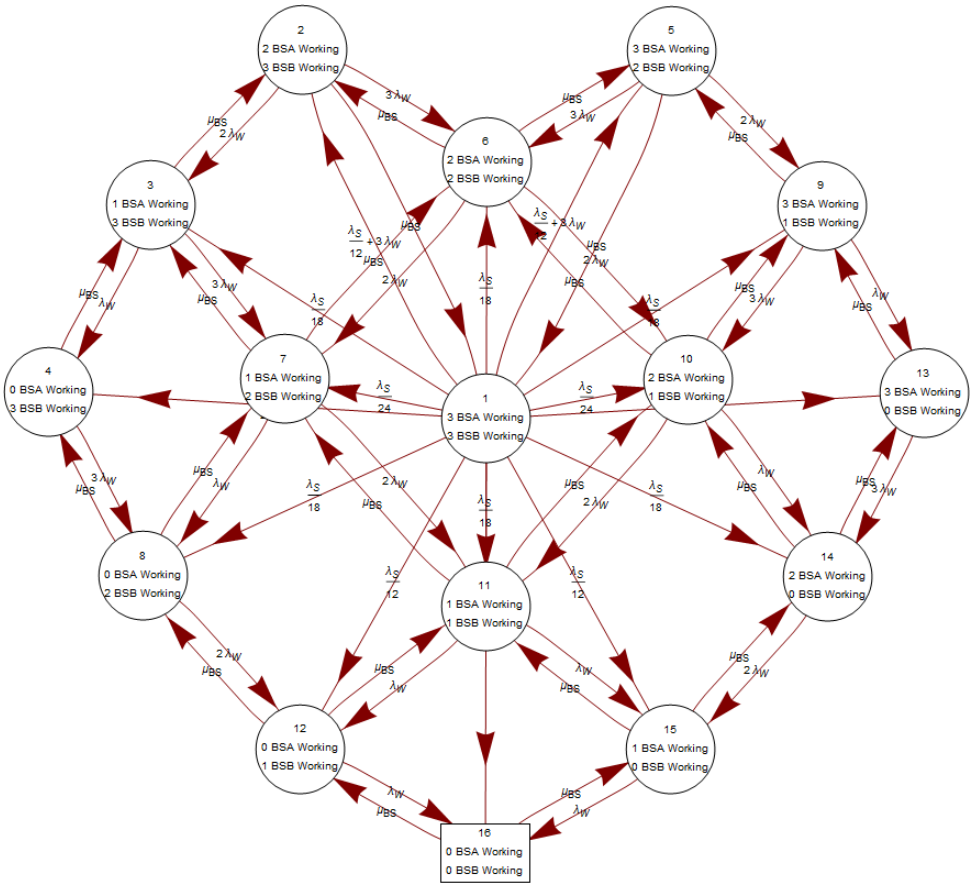

Figure 10.6: Markov dependability model of the smart grid from Figure 4.1 with BS failures caused by normal weathering and common cause BS failures caused by storms.

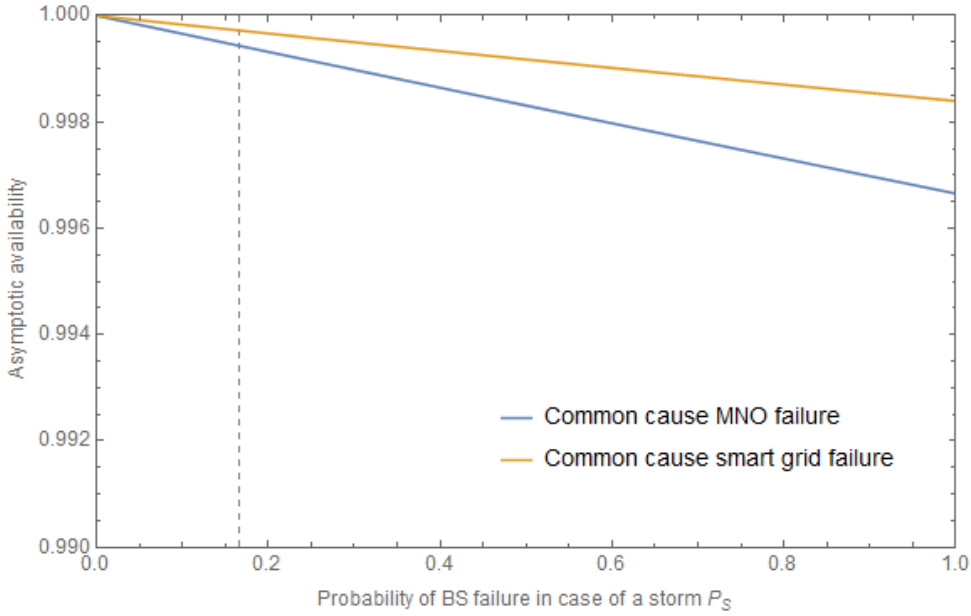

Figure 10.7: Plot of the asymptotic availability of the single MNO system from Figure 10.3 and the smart grid system from Figure 10.6 with respect to the probability of BS failure in case of a storm P_S. The dashed grid line shows the value of P_S used in use case 5.

$$A_{SG} = p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + p_7 + p_8 + p_9 + p_{10} + p_{11} + p_{12} + p_{13} + p_{14} + p_{15} + p_{16} = 0.999720 \quad (10.2)$$

10.3 Discussion

With dependability models created for the smart grid systems vulnerable to weathering and common cause BS failures caused by storms, a comparison of the systems with regard to asymptotic availability can be made. In the smart grids systems with common cause BS failures caused by storms the probability P_S affects how many BSs that will fail in case of a storm. Theoretically, if all the BSs in the system are vulnerable to common cause failure, e.g. if the storms are generally more destructive than portrayed in this use case or if the BSs have little protection against such hazards, that probability P_S would be higher. The plot in Figure 10.7 shows the asymptotic availability of the single MNO system from Figure 10.3 and the smart grid system from Figure 10.6 plotted with respect to the probability P_S.

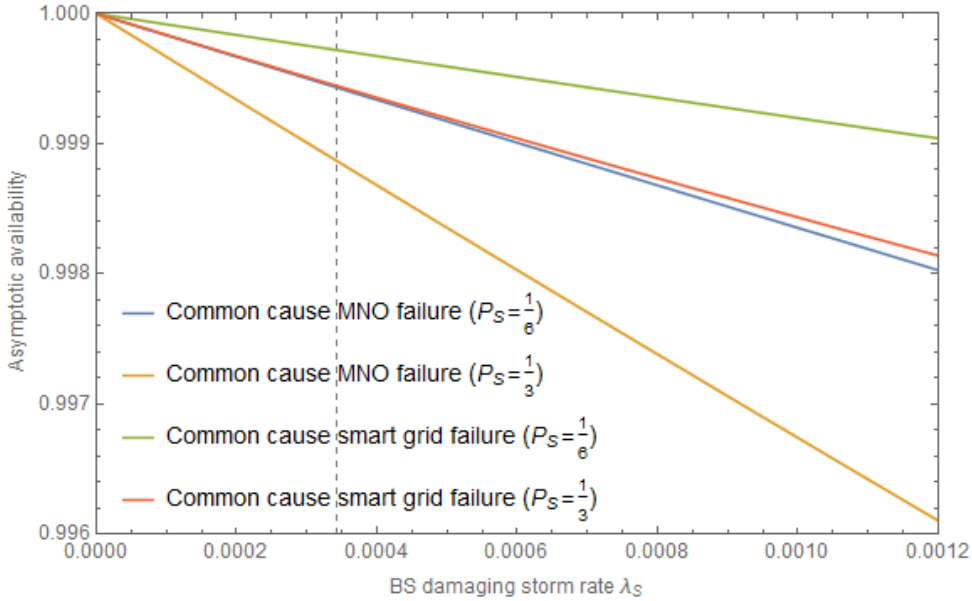

Figure 10.8: Plot of the asymptotic availability of the smart grid systems from Figure 10.3 with $P_S = \frac{1}{6}$, Figure 10.3 with $P_S = \frac{1}{3}$, Figure 10.6 with $P_S = \frac{1}{6}$, and Figure 10.6 with $P_S = \frac{1}{3}$ with respect to the BS damaging storm rate λ_S. The dashed grid line shows the value of λ_S used in use case 5.

It is seen from the plot in Figure 10.7 that the asymptotic availability of the two smart grid systems vulnerable to weathering and common cause BS failures has an apparent decrease in asymptotic availability if P_S is increased. Still, the difference in dependability of the two systems is relatively small. To get a better understanding of how the systems' asymptotic availability is affected by weathering and storms, the rate at which storms happen should also be regarded. The plot in Figure 10.8 shows the asymptotic availability of the same single MNO system from Figure 10.3 and the smart grid system from Figure 10.6, both with $P_S = \frac{1}{6}$, and $P_S = \frac{1}{3}$, plotted with respect to the rate of BS damaging storms λ_S.

The plot in Figure 10.8 shows that difference in asymptotic availability expand with an increased probability P_S and BS damaging storm rate λ_S. With $P_S = \frac{1}{3}$, meaning two failed BSs per storm in average, the difference between the single MNO system from Figure 10.3 and the smart grid system from Figure 10.6 stays about twice as big as when $P_S = \frac{1}{6}$. This observation gives an incentive to use multihomed SUs in areas especially prone to BS damaging storms.

Chapter 11
Use Case 6: Common Cause BS Failure with Common Repair

Presumably some BSs will have a stronger dependency to one another if they share a common weather exposed location or service, meaning they are more likely to fail together. Examples are BSs that are connected to the same mast or BSs that have power cables going through a common ditch prone to disturbances from road and construction work. In scenarios like this, when a common cause failure does not cause damage to the components failing themselves (the BSs), but a system the components are relying on (the ditch with power cables), only the one damaged system need to be repaired for all dependent components to be repaired. A scenario with several BSs failing due to a commonly used ditch is therefore a different type of common cause failure than BSs taking damage from a storm, where all BSs will have to be repaired independently.

In this use case the SUs are assumed to only be able to connect to two BSs. Both BSs will be subjected to normal failures from erosion due to weathering, and are in addition sharing a common ditch for power and ICT cables. The ditch is subjected to disturbances from road and construction work, potentially causing the power and ICT cables to take damage, again causing the BSs to fail. It is assumed that BS failures due to ditch disturbances do not occur at the same time as BS failures due to weathering because of the relatively low failure rates and high repair rates.

11.1 Single Base Station

For the sake of comprehension, a system where the SU can only connect to one single BS having cables through a ditch is presented first. The state space is defined as $\Omega = \{\{i\text{BS Working}, j\text{Ditch Intact}\} \mid i \in \{0,1\, j \in \{0,1\}$. The rates at which the ditch gets damaged so that the BS fails is λ_D, the repair rate of the ditch with cables is μ_D, and failure and repair rate for the BS are λ_W and μ_{BS}. Knowing all rates the dependability model becomes as seen in Figure 11.1.

With the steady state probabilities from the dependability model in Figure 11.1,

Figure 11.1: Markov dependability model of a single BS system with BS failures caused by normal weathering and a cable ditch for the BS.

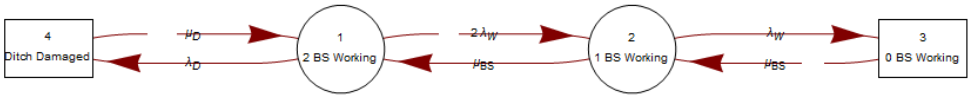

Figure 11.2: Markov dependability model of a BS system with two BSs from the same MNO, BS failures caused by normal weathering and a common cable ditch for the BSs.

denoted $\underline{p} = \{p_1, p_2, p_3\}$, the asymptotic availability A_{BS} of the single BS system with BS failures from erosion due to weathering and cable ditch disturbances is simply the same as the one steady state probability of the one working state, as seen in (11.1).

$$A_{BS} = p_1 = 0.992635 \tag{11.1}$$

11.2 Base Stations from a Single MNO

Now looking at a system assuming the SU can connect to two BSs sharing a cable ditch, where both BSs belongs to the same MNO and sharing one repair crew. The state space of the system is defined as $\Omega = \{\{i\text{BS Working}, j\text{Ditch Intact}\} \mid i \in \{0, 1, 2\, j \in \{0, 1\}\}$. The rate at which the ditch gets damaged so that the BSs fails is λ_D, and the repair rate of the ditch with cables is μ_D. Knowing the failure and repair rate for the BSs, λ_W and μ_{BS}, the dependability model becomes as seen in Figure 11.2.

With the steady state probabilities from the dependability model in Figure 11.2, denoted $\underline{p} = \{p_1, p_2, p_3, p_4\}$, the asymptotic availability A of the MNO system with BS failures from erosion and weathering and common cause BS failures from cable ditch damage is obtained by adding up the steady state probabilities of the working

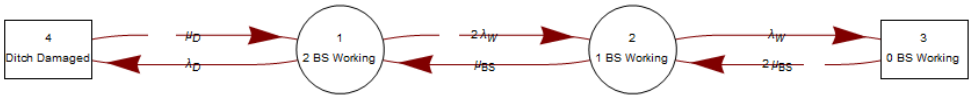

Figure 11.3: Markov dependability model of a BS system with two BSs from different MNOs, BS failures caused by normal weathering and a common cable ditch for the BSs.

states, as seen in (11.2).

$$A = p_1 + p_2 = 0.994902 \tag{11.2}$$

11.3 Base Stations from Both MNOs

Now looking at a system where the SU is multihomed and is able to connect to two BSs sharing a cable ditch. The two accessible BSs belong to different MNOs, MNO A and MNO B, with one repair crew per MNO. The state space of the system is defined as $\Omega = \{\{i\text{BS Working}, j\text{Ditch Intact}\} \mid i \in \{0, 1, 2\, j \in \{0, 1\}\}$. The rate at which the ditch gets damaged so that the BSs fails is λ_D, and the repair rate for the ditch with cables is μ_D. Knowing the failure and repair rate for the BSs, λ_W and μ_{BS}, the dependability model becomes as seen in Figure 11.3.

With the steady state probabilities from the dependability model in Figure 11.3, denoted $\underline{p} = \{p_1, p_2, p_3, p_4\}$, the asymptotic availability A of the system with BS failures from erosion due to weathering and common cause BS failures from cable ditch damage is obtained by adding up the steady state probabilities of the working states, as seen in (11.3).

$$A = p_1 + p_2 = 0.994907 \tag{11.3}$$

11.4 Discussion

With dependability models created for the BS systems with BS failures due to weathering and damaged cables because of ditch disturbances, the systems can be compared with regard to asymptotic availability. The plot in Figure 11.4 shows the asymptotic availability of the BS system with two BSs from the same MNO, as seen in Figure 11.2, and the BS system with two BSs from different MNOs, as seen in Figure 11.3, plotted with respect to the BS failure rate due to weathering λ_W.

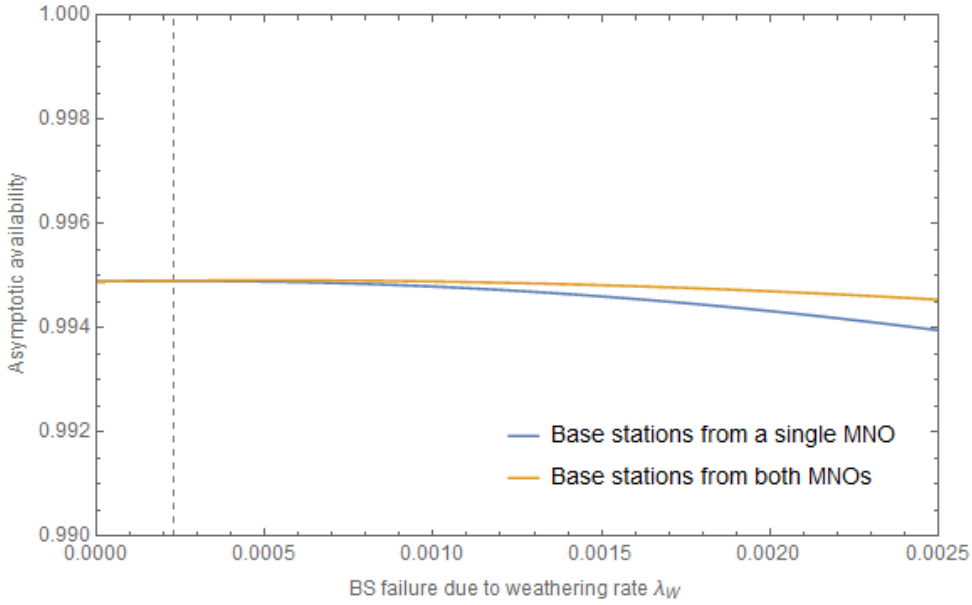

Figure 11.4: Plot of the asymptotic availability of the BS system with two BSs from the same MNO from Figure 11.2 and the BS system with two BS from different MNOs from Figure 11.3 with respect to the BS failure rate due to weathering λ_W. The dashed grid line shows the value of λ_W used in use case 5.

As expected, the system with BSs from both MNOs, and thus two repair crews, manages the increase in BS failure rate due to weathering λ_W better than the system with BSs from only one MNO, with λ_W going up to almost two BS failures per month. Looking at the asymptotic availability of the same two systems plotted with respect to the ditch damage rate λ_D reveals another observation. The plot with regard to λ_D is seen in Figure 11.5, where both systems are labeled BS system.

It is seen from the plot in Figure 11.5 that an increase in ditch damage rate λ_D has a much bigger effect on the systems than an increase in the BS failure rate due to weathering λ_W. The two systems' asymptotic availability stays approximately the same when plotting with respect to λ_D, giving an incentive for stakeholders in either system to focus on common cause BS failures, like damage to cables in ditches, rather than focusing on individual BS failures due to e.g. weathering.

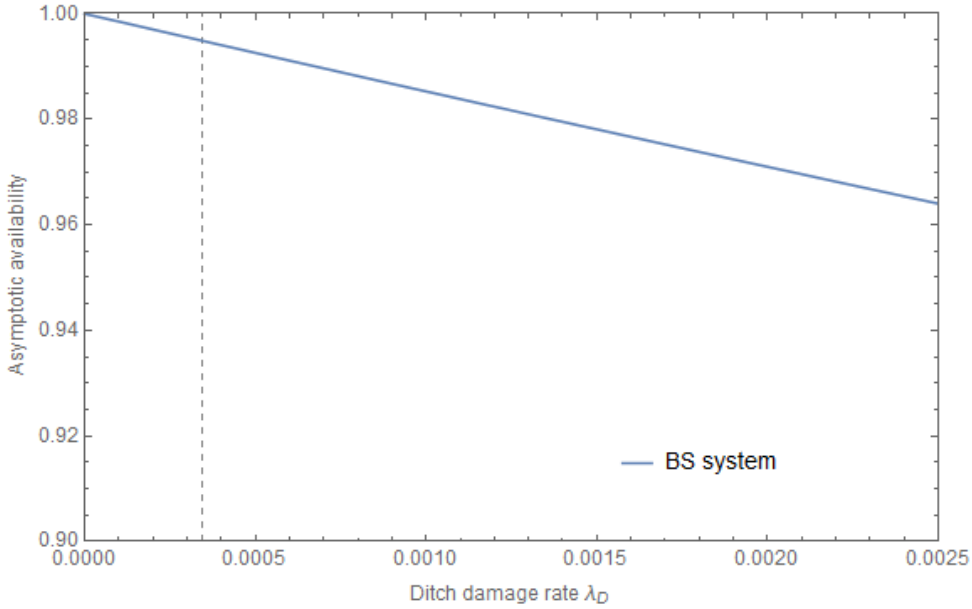

Figure 11.5: Plot of the asymptotic availability of the BS system with two BSs from the same MNO or from different MNOs with respect to the ditch damage rate λ_D. The dashed grid line shows the value of λ_D used in use case 5.

Chapter 12
Use Case Discussion

In the six use cases presented the asymptotic availability of several systems have been analysed, including systems with just a single BS, a single MNO and systems with two MNOs by using multihoming. Obviously smart grid systems can and will exist in a various of ways with different levels of complexity, and hence interdependencies in smart grid systems will exist in several ways as well. The six use cases presented shows proposals of how to make dependability models covering the presumably most realistic smart grid interdependencies and failures, and are meant as a basis for making dependability models of other and possibly more complex smart grids.

To get a better understanding of how to use the dependability modeling approaches proposed, in what scenarios they are fit, and where they fall short, this discussion chapter further analyse the modeling approaches from the use cases, elucidating potential shortcomings to avoid wrong use. Also, the numerical results from the use cases are compared to get an overview of the effect the investigated dependencies and failures have on smart grid systems' asymptotic availability.

12.1 Dependability Modeling

How the dependability models are created for the systems in the use cases is significant for the calculation of the systems' asymptotic availability. Making assumptions about and simplifications to the smart grid system is necessary when making dependability models, but can also lead to overly optimistic system dependabilities. Moreover, how the modeling approaches proposed scale to bigger and more advanced smart grid systems may be ambiguous. Some of the relatively simple modeling approaches presented could either not scale well with respect to smart grid system complexity, or the way in which disruptions propagate in the dependability models created may not work adequately on bigger smart grid systems. This section look at and discuss the assumptions made for the use cases and the dependability models created, and how the modeling approaches could be applied on other and potentially more complex

smart grid systems.

12.1.1 Use Case 1

In the first use case the issue of stress propagation between the DGs is solved with a DG stress constant s_{DG}, where if one of the DGs are failed the failure rate of the other DG is increased by s_{DG} becomes $(1 + s_{DG})\lambda_{DG}$. If a system including more DGs are to be modelled by the same approach there are two sensible ways in which the stress propagation solution with s_{DG} can scale; either by adding stress to all other DGs in the system when a DG is failed, or from a failed DG only adding stress to a number of adjacent DGs.

If choosing the stress propagation solution where stress is added to all other DGs when a DG fails, the DG failure rate including the added stress constant(s) s_{DG} must not become greater than the DG repair rate. For example, if five DGs have failed in a smart grid system and $(1 + 5s_{DG})\lambda_{DG} > \mu_{DG}$, other DGs will fail faster than already failed DGs are repaired, ending in the system being more or less trapped in a failed state. This problem can be solved by making it so that lesser DG stress is added by each new failed DG, e.g. the first failed DG add s_{DG} to the failure rate of the other DGs, the next failed DG add $\frac{1}{2}s_{DG}$, then $\frac{1}{4}s_{DG}$, and so on. Alternatively a failed DG can be assumed to only propagate stress to a number of adjacent DGs, effectively setting an upper limit for total stress added to DGs in the system.

12.1.2 Use Case 2

In the same way as the stress constant s_{DG} in the first use case, this use case utilize a load constant l_{BS} to realise propagation of congestion between the BSs. Again, if a system with more BSs is to be modelled by the same approach as used in this use case there are two ways in which the load propagation solution with l_{BS} can scale; either by adding load to all other BSs in the system when a BS is congested, or from a congested BS only adding load to a number of adjacent BSs.

Unlike with DGs, the propagation of congestion between BSs has clear bounds with regard to geographic distance between the BSs. If a BS becomes congested due to user crowding, only other nearby BSs will experience added load from the same crowd. In this way the most suitable way of scaling up the congestion propagation modeling approach is to only allow BSs to propagate congestion to other nearby BSs, and in this way also setting an upper limit for total load added to BSs in the system.

12.1.3 Use Case 3

As done with DG stress propagation in use case 1 and BS congestion propagation use case 2, this use cases realises propagation of BS malware with a malware constant

m_{BS}. Here the error rate of the BSs, not the BS failure rate, is increased as more BSs in the system get infected with malware. Because of this, the system is not subject to a situation where the system failure rate has become higher than the system repair rate, but could nonetheless end up in a situation where the system error rate is higher than the system error repair rate. This is not an inconceivable situation, where malware could indeed spread to, and exist at, all BS in a system.

If the dependability model of a smart grid system shows that the system could reasonably reach a state where all BSs are infected with malware, there are two ways of stabilising the system to a less infected state. Either the system can be assumed to run a periodic malware scan and removal by adding a low rate transition from all states to the one state with no BS malware infection, or the system can be assumed to upgrade its security SW and in this way decreasing the BS error rates and/or increasing the BS error repair rates.

12.1.4 Use Case 4

In use case 4 the issue of stress propagation between the DGs is solved with a DG stress constant s_{DG} in the same way as in use case 1, but here including a power grid control system in the smart grid. The up scaling of the modelling approach used in this use case can be done in the same manner as proposed for use case 1, with two ways in which the stress propagation solution with s_{DG} can scale; either by adding stress to all other DGs in the system when a DG is failed, or from a failed DG only adding stress to a number of adjacent DGs.

12.1.5 Use Case 5

This use case reveals some of the more complex dependability models among all the dependability models presented. Adding dimensions to a state space, e.g. by having the BSs in MNO A and the BSs in MNO B as two separate state space dimensions, adds complexity and possibly state space explosion. However, adding allowed values to the dimensions, e.g. by adding BSs to MNO A and/or MNO B, does add new states to the dependability model, but does not cause more complexity per se. In this way, using the modeling approaches presented will work fine for systems with only one or two MNOs, which are reasonable amounts of MNOs that a SU can connect to.

12.1.6 Use Case 6

In use case 6 a clear assumption made is that the system is assumed to never have BS failures due to weathering at the same time as BS failures due to ditch damage. In a small system like the one presented in use case 6, with only one or two BSs, this is a fair assumption because the chance of the two types of BS failures happening at the same time is negligible. However, if more BSs are added to the system the

chance of overlapping BS failures increase. The problem is easily solved by modeling the ditch dimension as done with the power grid control system dimension in use case 4, giving a two dimensional dependability model.

12.2 Numerical Results

The asymptotic availabilities obtained from the use cases give an indication on what dependencies and failures that are the most critical for smart grid systems. These observations give stakeholders an incentive to remove or loosen certain dependencies and to make barriers for certain failures. With targeted measures like this, resources for improving the dependability of smart grid systems can be used more wisely and with bigger effect.

Because some of the asymptotic availabilities A obtained from the use cases are very small they are presented as asymptotic unavailabilities U, computed $U = 1 - A$. Because of this, all numerical values from the use cases are in this section presented as asymptotic unavailabilities for easier comparison. Table 12.1 list the asymptotic unavailabilities obtained for all single MNO systems and smart grid systems utilizing both MNOs in the use cases. It is seen from the table that the single MNO systems have in general a higher asymptotic unavailability than the smart grid systems where both MNOs are utilized.

Some systems will presumably have a bigger incentive to utilize SU multihoming than others. What systems get the most benefit from utilizing multihoming can be obtained by computing the percentage difference d_r between the asymptotic availability of the single MNO systems A_1 and the smart grid systems utilizing both MNOs A_2 by using (12.1). Table 12.2 lists all percentage differences between the corresponding single MNO systems and smart grid systems utilizing both MNOs in the use cases.

$$d_r = \frac{|\Delta A|}{\sum \frac{A}{2}} \times 100 = \frac{|A_1 - A_2|}{(\frac{A_1 + A_2}{2})} \times 100 \tag{12.1}$$

From Table 12.1 it is seen that besides from the systems in use case 6, the single MNO systems in Section 6.1.1 and Section 9.2.1, from use case 1 and use case 4 respectively, have the lowest asymptotic availability of the single MNO systems presented. These systems also have the biggest increase in asymptotic availability if the SU is granted multihoming, as seen in Table 12.2 marked in red.

The second worst asymptotic availabilities belongs to the single MNO systems with BS power backup from Section 6.2.2 and Section 9.3.1, from use case 1 and use case 4 respectively, and the two systems from use case 5. Besides from these

Table 12.1: Overview of the asymptotic unavailabilities of the systems from the use cases. The red cells show the systems with the highest asymptotic unavailabilities, orange the next highest and yellow the third highest.

Use case	Section	Asymptotic unavailability
1	6.1.1	1.38×10^{-3}
	6.1.2	9.00×10^{-6}
	6.1.3	1.90×10^{-5}
	6.2.2	2.44×10^{-4}
	6.2.3	2.96×10^{-7}
	6.2.4	1.00×10^{-6}
2	7.2	2.20×10^{-5}
	7.3.1	5.60×10^{-10}
	7.3.2	6.48×10^{-10}
3	8.2	1.00×10^{-6}
	8.3.1	4.26×10^{-13}
	8.3.2	4.71×10^{-13}
4	9.2.1	1.38×10^{-3}
	9.2.2	9.00×10^{-6}
	9.2.3	1.90×10^{-5}
	9.3.1	2.44×10^{-4}
	9.3.2	2.98×10^{-7}
	9.3.3	1.00×10^{-6}
5	10.1	5.68×10^{-4}
	10.2	2.80×10^{-4}
6	11.2	5.10×10^{-3}
	11.3	5.10×10^{-3}

Table 12.2: Overview of the percentage differences d_r between the corresponding single MNO systems and smart grid systems utilizing both MNOs in the use cases. The red cells show the systems with the biggest percentage differences and yellow the next biggest.

Use case	Sections compared	d_r
1	6.1.1 - 6.1.2	0.1360%
	6.1.1 - 6.1.3	0.1350%
	6.2.2 - 6.2.3	0.0244%
	6.2.2 - 6.2.4	0.0243%
2	7.2 - 7.3.1	0.0022%
	7.2 - 7.3.2	0.0022%
3	8.2 - 8.3.1	0.0001%
	8.2 - 8.3.2	0.0001%
4	9.2.1 - 9.2.2	0.1367%
	9.2.1 - 9.2.3	0.1357%
	9.3.1 - 9.3.2	0.0244%
	9.3.1 - 9.3.3	0.0243%
5	10.1 - 10.2	0.0288%
6	11.2 - 11.3	0.0005%

systems having the second worst asymptotic availabilities, they have the second biggest increase in asymptotic availability if the SU is granted multihoming, as seen in Table 12.2 marked in yellow.

Even though the two systems from use case 6 has the two worst asymptotic availabilities of all the systems, then can not be directly compared with the systems from the rest of the use cases as they only utilize two BSs. Still, an observation from the numerical results from this use case stand, that using multihoming only minimally increases the system's asymptotic availability. Compared to the systems from use case 5 which also model common cause failures, it is seen that for common cause failures that allows individual repair of BSs multihoming gives a more noticeable effect.

Chapter 13
Conclusion

In the investigation in Part I, it was deduced that certain type combinations of dependencies and failures are more likely to happen in smart grids than others. More specific, *cascading failures over physical interdependencies*, *escalating failures over cyber interdependencies* and *common cause failures over geographic interdependencies* was deduced to be the most relevant sort of smart grid disturbances. Besides the three combinations of failure and dependency types mentioned, cascading failures over cyber interdependencies and common cause failures over physical and cyber interdependencies where found to be relatively relevant for smart grids as well.

Six use cases was presented, modeled and analysed in Part II. Using a defined smart grid system and Markov dependability modeling, all relevant combinations of dependencies and failures found in the investigation Part I was modeled and used to compute numerical results for the smart grid system's asymptotic availability. The use cases revealed that some combinations of dependencies and failures had probably bigger effects on the smart grid than others, namely cascading failures in the power grid and common cause BS failures due to natural events like storms or human caused events like maintenance disturbing the operation of the BSs indirectly.

Besides pointing out what types of dependencies and failures in digital ecosystem that should be in focus for stakeholders, the use cases and the dependability models made are intended as a guideline for dependability modeling in future digital ecosystems like smart grids. Based on the findings from the use cases Table 13.1 lists realistic dependencies in smart grids and suggest what modeling that should be used to deal with them.

The findings and insights from the investigation and use cases presented have answered to the objective behind this thesis, but have also revealed some new questions to be answered; how does Markov dependability modeling in smart grids hold up against other modeling approaches, how accurate are the results obtained, and what vulnerabilities are brought into smart grids with added ICT?

Table 13.1: Relevant dependencies and failures in smart grids and suggested dependability modeling approaches for analysing them.

System	Suggested modeling approach
Cascading power grid failure	Have the power grid components or subsystems failing as a dimension in the state space, use a constant for increasing failure rates to realize propagation of failure in the power grid and if relevant, use a constant for decreasing repair rate in case of telecommunication interdependency.
BS power backup	Assume negative exponential distribution on power backup and make dependability models for single BSs. Use the failure rate of the single BS dependability models to create a dependability model for the smart grid.
Cascading BS congestion	Have the BSs failing as a dimension in the state space and use a constant for increasing failure rates to realize propagation of BS congestion failure in the smart grid.
Cascading BS malware	Have the components getting infected as a dimension in the state space and use a constant for increasing failure rates to realize propagation of malware in the smart grid. Remember that malware can exist and propagate without components failing per se.
Power grid control system	Obtain the asymptotic availability of the power grid control system and use it to set up new failure rates for the components or subsystems being controlled; normal failure rate times the control system asymptotic availability plus escalated failure rate times control system asymptotic unavailability.
Storm causing common cause BS failure	If realistic, assume all BS are repaired between common cause failures and add a transition from the OK state to all states with failed BSs. The transition rate is the rate of common cause failures times the probability that the failure leads to the specific state pointed to.
BS dependent on a common system	If realistic, assume all BS are repaired between failures in the common system and let the common system have its own failure and repair rate.

In the use case analysis done here, Markov modeling have been used for computing numerical results. To get an even better understanding of how dependencies and failures affect digital ecosystems, a proper discrete-event simulation of the dependency and failure types could have been done, which would also work as a quality control of the results obtained from the Markov dependability models. A discrete-event simulation has less restrictions than Markov models, allowing the smart grid system to be analysed with fewer assumptions and, if needed, more state space dimensions, where Markov models are often subjected to state space explosion.

The threat of malware in smart grids is uncertain, where the more ICT solutions that are integrated into smart grids, the more ways the smart grid can be affected by malware. To be prepared for possible cyber attacks and malware in future smart grids a thorough study on ICT dependencies and failures in future smart grids should be performed.

References

[AFÅ+14] Camilla Aabakken, Hege Sveaas Fadum, Astrid Ånestad, Fredrik Hageengen, and Ragnhild Aker Nordeng. Avbrotsstatistikk 2013 [Outage Statistics 2013]. Technical Report 74, Noregs vassdrags- og energidirektorat, November 2014.

[Ald03] David Louis Alderson. *Congestion-Induced Collapse in Networks: Managing Failure Cascades in Complex Systems and Infrastructure Protection.* PhD thesis, Stanford University, Stanford, CA, USA, May 2003.

[ALRL04] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33, January 2004.

[Ami00] Massoud Amin. National Infrastructure as Complex Interactive Networks. In *Automation, Control and Complexity: An Integrated Approach*, pages 263–286. John Wiley & Sons, August 2000.

[ASC12] Arizona-Southern California Outtages on September 8, 2011: Causes and Recommendations. Technical report, FERC/NERC, April 2012.

[BC07] Harold Boley and Elizabeth Chang. Digital Ecosystems: Principles and Semantics. *2007 Inaugural IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2007)*, pages 398–403, February 2007.

[BCH+12] Chris Barrett, Karthik Channakeshava, Fei Huang, Junwhan Kim, Achla Marathe, Madhav V. Marathe, Guanhong Pei, Sudip Saha, Balaaji S. P. Subbiah, and Anil Kumar S. Vullikanti. Human Initiated Cascading Failures in Societal Infrastructures. *PLOS ONE*, 7(10), October 2012.

[BN03] Rainer Bacher and Urs Näf. Report on the Blackout in Italy on 28 September 2003. Technical report, Swiss Federal Office of Energy (SFOE), November 2003.

[BPP+10] Sergey V. Buldyrev, Roni Parshani, Gerald Paul, Harry Eugene Stanley, and Shlomo Havlin. Catastrophic Cascade of Failures in Interdependent Networks. *Nature*, 464:1025–1028, April 2010.

[CBK07] Yanyan Chen, Michael G. H. Bell, and Ioannis Kaparias. Reliability Analysis of Road Networks and Preplanning of Emergency Rescue Paths. In *Critical*

Infrastructure; Reliability and Vulnerability, Advances in Spatial Science, pages 173–196. Springer Berlin Heidelberg, 2007.

[CDC10] Cybersecurity Through Real-Time Distributed Control Systems. Technical report, Oak Ridge National Laboratory, February 2010.

[EHHP12] Peder J. Emstad, Poul E. Heegaard, Bjarne E. Helvik, and Laurent Paquereua. *Dependability and Performance in Information and Communication Systems*. Tapir Akademisk Forlag, Nardovegen 12, 7005 Trondheim, 6 edition, June 2012.

[FH11] Eirik Larsen Følstad and Bjarne E. Helvik. Failures and Changes in Cellular Access Networks; A Study of Field Data. In *2011 8th International Workshop on the Design of Reliable Communication Networks (DRCN)*, pages 132–139. IEEE, October 2011.

[Fis06] David A. Fisher. An Emergent Perspective on Interoperation in Systems of Systems. Technical Report CMU/SEI-2006-TR-003, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, March 2006.

[FRS07] Final Report - System Disturbance on 4 November 2006. Technical report, Union for the Co-ordination of Transmission of Electricity (UCTE), January 2007.

[Hel09] Bjarne E. Helvik. *Dependable Computing Systems and Communication Networks; Design and Evaluation*. Tapir Akademisk Forlag, Nardovegen 12, 7005 Trondheim, January 2009.

[HM06] Åke J. Holmgren and Staffan Molin. Using Disturbance Data to Assess Vulnerability of Electric Power Delivery Systems. *Journal of Infrastructure Systems*, 12(4):243–251, December 2006.

[Int11] International Energy Agency (IEA). *Technology Roadmap: Smart Grids*, 9 rue de la Fédération, 75739 Paris Cedex 15, France, April 2011.

[KB09] Daniel Kirschen and François Bouffard. Keeping the Lights On and the Information Flowing. *Power and Energy Magazine*, 7(1):50–60, January 2009.

[KC06] Samuel T. King and Peter M. Chen. SubVirt: Implementing Malware with Virtual Machines. In *2006 IEEE Symposium on Security and Privacy*, pages 313–327, May 2006.

[LKK07] Jean-Claude Laprie, Karama Kanoun, and Mohamed Kaâniche. Modelling Interdependencies Between the Electricity and Information Infrastructures. In *Computer Safety, Reliability, and Security*, volume 4680 of *Lecture Notes in Computer Science*, pages 54–67. Springer Berlin Heidelberg, September 2007.

[Mal10] Rakesh Malhotra. Energy Management & Backup Unit for Telecom Base Stations. In *32nd International Telecommunications Energy Conference (INTELEC)*, pages 1–5. IEEE, 2010.

[Mei12] Haibo Mei. *Improving Relay Based Cellular Networks Performance in Highly User Congested and Emergency Situations.* PhD thesis, School of Electronic Engineering and Computer Science, Queen Mary, University of London, January 2012.

[PSO04] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Technical report, U.S.-Canada Power System Outage Task Force, April 2004.

[RBM09] Hafiz Abdur Rahman, Konstantin Beznosov, and Jose R. Marti. 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):220–244, May 2009.

[RPK01] Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*, 21:11–25, December 2001.

[SOK+13] Seppo Sierla, Bryan M. O'Halloran, Tommi Karhela, Nikolaos Papakonstantinou, and Irem Y. Tumer. Common Cause Failure Analysis of Cyber–Physical Systems Situated in Constructed Environments. *Research in Engineering Design*, 24(4):375–394, June 2013.

[WH13a] Jonas Wäfler and Poul E. Heegaard. A Combined Structural and Dynamic Modelling Approach for Dependability Analysis in Smart Grid. In *Proceedings of the 28th Annual ACM Symposium on Applied Computing*, SAC '13, pages 660–665. Association for Computing Machinery (ACM), 2013.

[WH13b] Jonas Wäfler and Poul E. Heegaard. Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability. In *Advances in Communication Networking*, volume 8115 of *Lecture Notes in Computer Science*, pages 185–196. Springer Berlin Heidelberg, 2013.