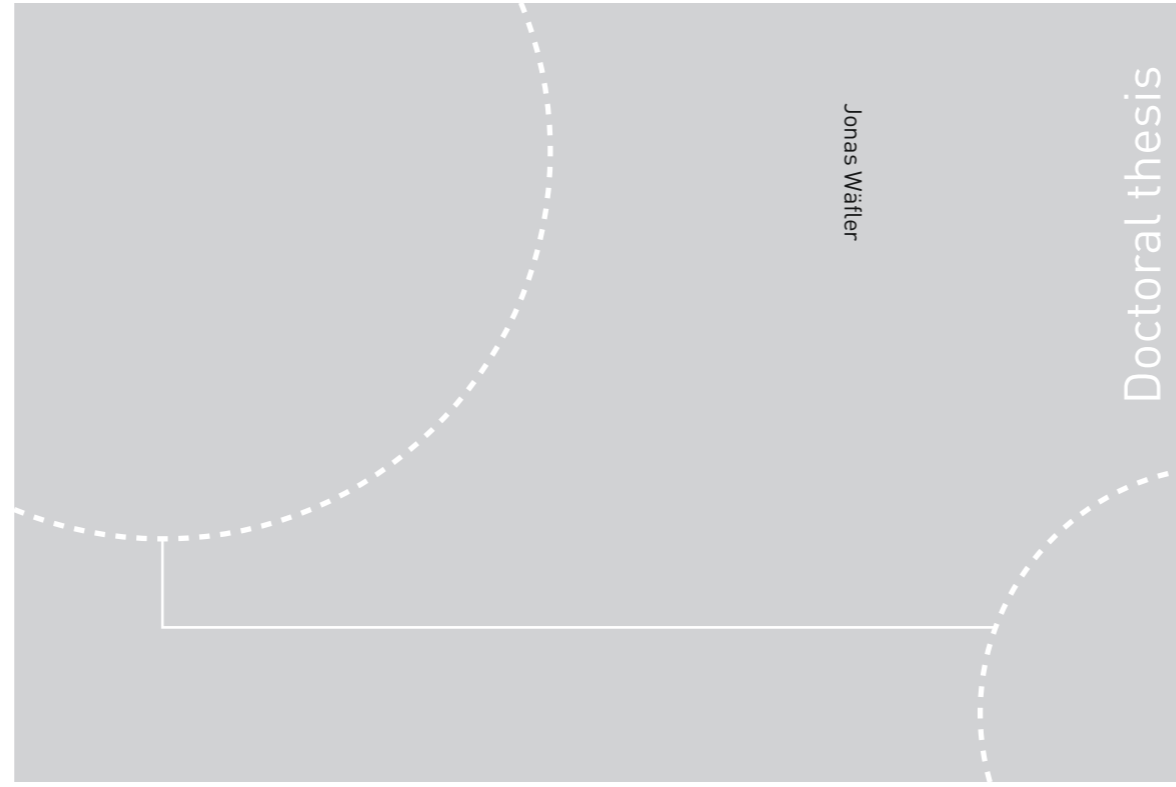


ISBN 978-82-326-1458-5 (printed ver.)  
ISBN 978-82-326-1459-2 (electronic ver.)  
ISSN 1503-8181



Doctoral theses at NTNU, 2016:60

Jonas Wäfler

# Modeling and Analysis of Dependability and Interdependency Failures in Smart Grids

Study on how the wide usage of ICT changes the Dependability in the future Power Grid

 **NTNU**  
Norwegian University of  
Science and Technology

Doctoral theses at NTNU, 2016:60

 NTNU

**NTNU**  
Norges teknisk-naturvitenskapelige universitet  
Thesis for the Degree of  
Philosophiae Doctor  
Faculty of Information Technology,  
Mathematics and Electrical Engineering  
Department of Telematics

 **NTNU**  
Norwegian University of  
Science and Technology

Jonas Wäfler

# Modeling and Analysis of Dependability and Interdependency Failures in Smart Grids

Study on how the wide usage of ICT changes  
the Dependability in the future Power Grid

Thesis for the Degree of Philosophiae Doctor

Trondheim, March 2016

Norwegian University of Science and Technology  
Faculty of Information Technology,  
Mathematics and Electrical Engineering  
Department of Telematics



Norwegian University of  
Science and Technology

**NTNU**

Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Information Technology, Mathematics and Electrical Engineering  
Department of Telematics

© Jonas Wäfler

ISBN 978-82-326-1458-5 (printed ver.)  
ISBN 978-82-326-1459-2 (electronic ver.)  
ISSN 1503-8181

Doctoral theses at NTNU, 2016:60

Printed by NTNU Grafisk senter

*To Debora,  
Anouk and Moritz*



---

## Abstract

The transition from the current electrical power grid towards a smart grid is driven by new technologies and services. Traditional dedicated power grid components are exchanged with more powerful and highly configurable devices that are interconnected and help monitoring and controlling the power grid. The power grid is a critical infrastructure with high dependability requirements. The pervasive use of information and communication technology (ICT) to support the operation in the smart grid creates a complex interdependent system in which the dependability of the ICT systems plays an important role for the overall dependability. Additionally, interdependent system-of-systems feature new failure modes not found in simple systems. Therefore, it becomes crucial to understand and address the dependability issues in the smart grid in order not to risk a decreasing dependability with the introduction of new technology.

The objective of this thesis has been to analyze how the dependability of the power grid changes with the introduction of smart grid technologies, to propose new dependability models and propose operational support mechanisms for the control center to detect and master the expected dependability issues in the smart grid. The first step of the research was to conduct literature studies to find new dependability challenges in the smart grid. Based on that, the consequences of these new challenges are assessed with the help of analytical models and simulations.

My findings show that there are several challenges such as cascading and escalating failures, latent errors and a risk of automation waiting when transitioning towards a smart grid. The qualitative and quantitative analysis show that these effects can have a strong impact on the total dependability of the smart grid and need to be considered. The analysis also shows that smart services like demand response or automatic detection and isolation of failures can help improving the dependability if implemented with the right supporting measures. As a conclusion from the analysis, I give a list of guidelines for the control center on how to address the future challenges. One of the central advices from this thesis to the electrical utilities is, that they should try to thoroughly understand their specific

interdependencies by analyzing their systems, processes and organizational structure. The next step is then to create awareness inside the company and invest in preparedness and mitigation strategies.

Overall, this thesis contributes to the discussion on new dependability challenges in the smart grid, the definition of realistic use cases illustrating how they might affect the system, the quantification of their consequences, and the discussion on how the utilities might address these new challenges.

---

## Acknowledgments

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) for partial fulfilment of the requirements for the degree of philosophiae doctor. This doctoral work has been performed at the Department of Telematics with Professor Poul E. Heegaard from the Department of Telematics as main supervisor and Adjunct Professor Kjell Sand from the Department of Electric Power Engineering as co-supervisor.

This work has been funded by the project *Next Generation Control Centre*, a project co-funded by the Norwegian University of Science and Technology and industry partners under the umbrella organisation *Norwegian Smartgrid Centre*.<sup>1</sup>

Several people have directly or indirectly contributed to this work. First of all, I would like to thank my supervisor Poul E. Heegaard for his support: thanks for always having an open door and having time for my questions, it has been a great pleasure working with you. Special thanks go to Bjarne E. Helvik for some good discussions, they helped me to see my project from a different angle. I would like to thank Kjell Sand and Rolf Michelsen for managing the *Next Generation Control Centre* project.

Many thanks go to: Maciej Wielgosz, Joe-Kai Tsay, Gergely Biczók for the many enjoyable lunch breaks and discussions; Vijay Venu Vadlamudi for getting me started with academic writing; my room mates Maria Bartnes Line, Joakim Klemets, Katrien De Moor, Gianfranco Nencioni, Doreid Ammar, Mauritz H. Panggabean for the good discussions.

Finally, life is much more than research. I would like to use this opportunity to thank my parents for their support throughout my life. This thesis is dedicated to my wife Debora and our children Anouk and Moritz, I would like to thank them for their love, support and patience: You make life worth living!

Jonas Wäfler,  
Trondheim, December 2015

---

<sup>1</sup><http://www.smartgrids.no/english/>





---

# Contents

Abstract . . . . .	iii
Acknowledgments . . . . .	iv
<b>I Thesis Introduction</b>	<b>1</b>
<b>1 Introduction</b>	<b>3</b>
1.1 Motivation . . . . .	4
1.2 Note on Terminology . . . . .	5
1.3 Research Questions . . . . .	7
1.4 Scope . . . . .	8
1.5 Research Method . . . . .	8
1.6 Included Papers . . . . .	10
1.7 Thesis Structure . . . . .	13
<b>2 State of the Art</b>	<b>15</b>
2.1 Challenges and Modeling . . . . .	15
2.2 Analysis . . . . .	19
<b>3 Contribution and Discussion</b>	<b>23</b>
3.1 Contribution . . . . .	23
3.2 Discussion . . . . .	26
<b>4 Concluding Remarks</b>	<b>33</b>
<b>References</b>	<b>35</b>
	vii

<b>II Included Papers</b>	<b>41</b>
Paper A Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability	43
Paper B A Combined Structural and Dynamic Modelling Approach for Dependability Analysis in Smart Grid	57
Paper C Structural Dependability Analysis in Smart Grid under Simultaneous Failures	65
Paper D Quantifying Influence of Strategies and Network Properties in Repairing Simultaneous Failures in Smart Grid	73
Paper E How to Use Mobile Communication in Critical Infrastructures: A Dependability Analysis	87
Paper F Interdependency in Smart Grid Recovery	99
Paper G Managed Dependability in Interacting Systems	109
<b>Appendix</b>	<b>141</b>
A Details on Downtime-Frequency Curve and ENS Extension	143

PART I

---

**THESIS INTRODUCTION**



---

## Introduction

The industrialization and the emergence of the information age has put the electrical power system into a central position in our society. Our daily life depends strongly on a reliable electrical power supply; a large blackout may lead to problems in communication networks, in the transportation sector, in the financial sector and basically in any field with machinery or equipment relying on supply from the power grid.

Everything indicates that the electrical power system has to undergo major changes over the course of the next decades to adapt to new challenges both on the supply and demand side. On the supply side, we see an increasing use of renewable energy sources around the world because of a desire of either reducing CO<sub>2</sub> emissions, stepping down the usage of nuclear energy, reducing energy imports, or a combination of it. The power production with renewable energy sources is in many cases less predictable than with traditional energy sources making the operation of the grid more challenging. At the same time, the demand side is also bound to change in the future. Electrical vehicles are on the rise and increase both the energy and power consumption of household customers, which change the load pattern and might push the distribution grid, the low voltage part of the power grid, to the margins of its capacity. Additionally, it is expected that some consumers become *prosumers*, i.e. they possess a small power production facility in the form of for example photovoltaic cells. A prosumer may choose to supply or demand power from the grid depending on its needs, its production, and the current energy price and is changing thereby the load pattern, too.

The mentioned challenges differ between countries but there is unanimity that they should be addressed by making the power grid *smarter*, thereby creating the *smart grid*. The added smartness refers to an increased use of monitoring and controlling devices in the power grid, especially in the lower voltage part, allowing for a more accurate state estimation of the grid and a more detailed control of it. This opens up for automation of processes and for new services like for example remote controlling certain loads.

We can loosely split the smart grid into the power grid and the supporting information and communication technology (ICT) system. Both depend strongly on each other's reliable service: one relies on power supply, the other on monitoring data and a channel to control devices. Together they build an interdependent system-of-systems. These kind of interconnected systems are not only more complex than more independent systems but because of the mutual interdependencies, they have additional failure modes as described in Rinaldi et al. (2001).

Already today relies the power grid strongly on ICT for operation. The analysis of past incidents by Kirschen & Bouffard (2009) shows that these interdependency effects had an important role in several large outages, either they were partly caused by a failure in the ICT system or a power grid failure was made more severe because the ICT system ceased to work. Xie et al. (2002) analyzed disturbances in the US power grid from 1979 to 1995 and state that "*problems in real-time monitoring and operating control system, communication system, and delayed restoration contribute to a very high percentage of large failures*". Because of the nature of the smart grid, the interdependencies between the two systems is going to further increase and the question becomes: how can this challenge be addressed?

## 1.1 Motivation

Reliability, the term used for dependability in power engineering, has always played a central role in the power grid. In the future grid, the smart grid, it has at least the same importance. This is reflected by the mentioning of the term *reliability* in most smart grid reports, for example the European Commission (2006) states in there vision that smart grids need to be "*flexible, accessible, reliable and economical*". The Electric Power Research Institute (EPRI) in the US defines a smart grid as follows: "*A Smart Grid is one that incorporates information and communications technology into every aspect of electricity generation, delivery and consumption in order to minimize environmental impact, enhance markets, improve reliability and service, and reduce costs and improve efficiency*" (EPRI, WEB). I.e. the use of ICT shall *improve reliability* by means of process automation, and an increased amount monitoring and controlling infrastructure.

The National Energy Technology Laboratory (NETL) (2010) analyzes the benefits of implementing smart grid technologies in a qualitative way and they find positive effects in various areas such as dependability and safety. However, it is assumed that the technologies function flawlessly when needed or that failures in the ICT infrastructure have no major impact on the total smart grid dependability. But is this true?

It is difficult to say if the assumption is justified or overconfident; it needs further investigation. Experience shows that ICT systems indeed fail and it can be assumed that they will also do so in the future. In the best case, a failure in the ICT system/service just negates its positive effects and brings the system to the same state as before the introduction of that specific ICT system/service and the dependability may drop at most to that past level. However, ICT can potentially fail in more ways than that, for example by sending faulty commands which may lead to catastrophic consequences. Additionally, the increased interdependencies introduce new failures as well, as mentioned above. The question is if all this still leaves a positive dependability contribution of ICT or not? This question cannot be answered directly because there are many parameters that have to be taken into account such as properties of the specific power grid, the ICT system, their interconnections and interdependencies etc. The North American Electric Reliability Corporation (NERC) is aware of this and states: *“The main challenge for the envisioned smart grid infrastructure is to integrate smart grid devices and systems while maintaining reliability”* (NERC Report, 2010).

What we can state after this introduction is, that a smart grid is more complex than a traditional power grid and may possess different failure modes. Faulty ICT systems and interdependency effects between ICT and the power grid have to be carefully analyzed and they have to be included in the dependability analysis, otherwise the results may be inaccurate and could lead to false conclusions about the system.

And as a final note: It is probable that the total dependability is increased by the introduction of some new smart grid technologies based on ICT, but there is more to dependability than just average values like steady-state availability. Depending on the specific scenario, other properties are more important such as the shape of the distribution, extreme values or the specific date or time of an outage. For example, Norwegians heat their households primarily with electricity. One long outage may have a more adverse effect for the customer than several shorter outages.

## 1.2 Note on Terminology

New terms are usually defined whenever they are used the first time. The following terms take a very central role in the thesis and also the introduction, therefore, I give some clarification about them already now.



### 1.2.1 Dependability, Reliability, Availability and more

The terms *dependability*, *reliability* and *availability* are used differently in the ICT domain and in power engineering. In the former, the definitions of Avizienis et al. (2004) are widely accepted, which uses *dependability* as an umbrella term defined as "*the ability to avoid service failures that are more frequent and more severe than is acceptable*". It comprises several quantifiable attributes among others *availability* and *reliability*, which are defined as "*readiness for correct service*" and "*continuity of correct service*", respectively.

In power engineering the definitions from IEEE/CIGRE Joint Task Force on Stability Terms and Definitions (2004) are widely employed. *Reliability* is used as umbrella term or similar to *availability* as defined above. It is expressed through *Adequacy* and *Security*, defined as "*ability of the power system to supply the aggregate electric power*" and "*ability of the power system to withstand sudden disturbances*", respectively. Additionally, the term *stability* refers to the continuance of intact operation following a disturbance.

The terms are well defined within their field but it can get ambiguous when the two fields meet. To avoid confusion, I use whenever possible the former definitions by Avizienis et al. (2004), which are used in ICT, even if referring to the power grid.

### 1.2.2 Smart Grid

The term *Smart Grid* is widely used in research, governmental commissions and newspapers and while there exist various definitions, most of them resemble each other. The European technology platform defines a smart grid for example as "*an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies.*" (European Commission, 2010). EPRI's definition, given in Section 1.1, is very similar and has a similar high abstraction level.

In literature, the term smart grid is generally used in two different ways. First, it is used to describe a vision for the future power grid. This vision is characterized not by specific technologies but rather by certain functionalities, such as active consumer participation, and accommodation of a wide range of different power generation and storage options (National Energy Technology Laboratory (NETL), 2009). Visions are usually used to set a direction but it is not expected to achieve them. Second, the term smart grid is used in a more pragmatic way to denote the next generation power grid, i.e. the power grid that is going to be implemented in about 10-20 years, which incorporates certain aspects of the smart grid vision. Certain authors use two different terms to distinguish between the two

cases (Vadlamudi et al., 2014), but more often than not the term *smart grid* is used without an explicit definition, often implying the latter definition. In this thesis, the term smart grid is mostly used in the latter way, i.e. standing for the *future power grid* or the *next generation power grid*; these terms are used synonymously with *smart grid* throughout the thesis.

It is important to note that power grid challenges vary strongly between countries and continents. The challenges depend on factors such as distribution of consumer types, consumption patterns, the type of power production, age of infrastructure and its reliability, and governmental policies. Therefore, smart grids may look very differently throughout the world.

### 1.3 Research Questions

The objective of my research is to understand how the dependability of the power grid changes with the introduction of the smart grid technologies in order to propose guidelines for the grid operators, on how to address these new issues and to be prepared for the future challenges in the smart grid.

This can be broken down into the following research questions leading towards an answer of the objective:

#### **RQ1 Challenges and Models: What are the new dependability challenges in the interdependent smart grid and how can they be modeled?**

The aim of RQ1 is to describe how the dependability analysis differs between the current power grid and the smart grid. The focus lies on new dependability threats and new potential faults that are introduced by the new add-ons to the current power grid and how they may manifest in the future. The second step is to define dependability models, which allow to analyze the smart grid including the new potential threats. The aim is not to make one big model, but rather to concentrate on particular threats and model them. The outcome are several models, which can be used to analyze specific scenarios.

#### **RQ2 Impact Analysis: What impact do the future challenges have on the dependability of the smart grid?**

The aim of RQ2 is to quantify the impact the new threats and failures have on the dependability of the smart grid. For this, scenarios depicting relevant future scenarios are created and analyzed. Additionally, it includes the assessment of how future smart grid services can contribute to face the future challenges.

The research questions build on each other as shown in Figure 1.1. The outcome of RQ1 is a number of threats specific to the smart grid and models. RQ2

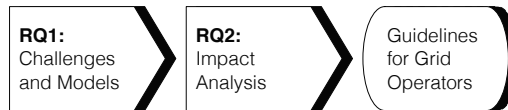


Figure 1.1: Relation of the research questions and the overall objective.

can be answered with the help of the new models from RQ1 and based on the results and their discussion, guidelines can be formulated, thus answering the overall objective.

## 1.4 Scope

In this thesis I focus on dependability challenges caused by the interdependency and interaction of the power grid and the supporting ICT system. Both systems come from different domains and there is a lot of research about various aspects of both of them. For the thesis I have to limit myself on a certain aspect and choose a certain abstraction of the systems. I primarily limit myself to the dependencies between the systems because I am most interested in the superordinate new challenges of the systems. Related topics such as performance analysis and ICT security are outside the scope of this work.

I use abstraction to hide details that are not of major importance to the study. For example, the power grid is either considered as a black box supplying power or only its structure is considered. The dynamics in the power grid such as voltage fluctuations are not considered because they are not central for answering the research questions. In the same way, the ICT system is only considered in as much details as necessary in the different studies. Details such as protocols are not included when not needed to analyze the functional dependencies.

The objective is not to develop an all-purpose smart grid dependability model but rather to concentrate on specific aspects and services and analyze what changes they may bring and how the control center may prepare for them.

## 1.5 Research Method

In order to answer RQ1 I have conducted a broad literature study yielding a list of potential future challenges, which are then evaluated for their relevance in smart grid. Subsequently, I have created use cases for the future smart grid based on the criteria that they both depict an important part of the future grid and illustrate the effect future challenges can have on systems.

Depending on the objective and the complexity of the system, I have chosen different modeling approaches. One of the main problems in modeling is the right choice of abstraction. The motto *as few details as possible but as many as needed* is a good but rather vague guide. I tried to solve this in various ways: modeling bottom-up or top-down, and also modeling the structure or a specific process. I started out with a bottom-up approach, which allows to create a detailed model of the system and it allows to use state-based and structural models to qualitatively assess interdependencies in the system. The approach is based on the concept of *errors* that are in the system but do not manifest themselves as failures. This is defined in Avizienis et al. (2004); Laprie et al. (2007) uses it in a smart grid model under the name *latent error*. In the context I have used them, these models remain comprehensible and provide a good basis for discussion. They are only used to model single components or the whole system in a very high abstraction level. Thus, the complexity of the model is limited. When using this approach for modeling a larger system in a quantitative way, issues such as state explosion occur and have to be solved.

For *Paper C* and *Paper D*, I used a top-down approach with focus on the structural dependability of the systems, considering only the topology and some special properties of the system. The dynamics in the power grid are ignored, which is a strong abstraction but it shows what the system can achieve if all the power engineering challenges are successfully met. The structural analysis is conducted on a real-world regional power grid in Norway. I was provided with the topology from a utility in our project and digitized it by hand. Information about the power grid are very sensitive, therefore, I only received the topology without information about customer types or consumption and production facilities. In *Paper D*, I additionally use random networks with node degree distribution following an exponential distribution, because it has been indicated by Rosas-Casals et al. (2007) that the European transmission networks possess this property. I used information from the Norwegian regulator to make educated guesses as described in the papers. The analysis itself is then conducted in the form of a Monte Carlo simulation in Mathematica (Wolfram Research, 2012).

Another high abstraction level is used for modeling the mobile networks in *Paper E*. Each network is treated as a black box and is either working or not working. The reason for this modeling approach is that this is how a subscriber sees the network, it has no information about the detailed state of the network. The measurement data from the study by Kvalbein (2013) serve as a starting point. The dependency between the two mobile networks is given implicitly in the study, however, its nature is unspecified as the networks are considered as black boxes and no details about the networks are known. The relation between the networks could be modeled as a common cause failure or with load sharing, i.e. in case of a failure in the first network the second network is subject to increased stress due to

load sharing. I have chosen the former, because statistics on incidents in mobile network indicate that at least half of the incidents, in remote areas even up to 90 %, are caused by power failures or failures in a leased line (Følstad & Helvik, 2011). Those failures can potentially cause a simultaneous failure in another network and thereby a common cause failure.

*Paper F* and *Paper G* analyze each a specific process in the power grid and for the modeling I use SAN (stochastic activity network (Sanders & Meyer, 2001)) and a Markov model, respectively. SAN is an extension of stochastic petri nets and has the advantage, that it can prevent state explosion issues by hiding details in a comprehensible visual model. It remains readable even when considering multiple failures like in my study. The model cannot be solved directly, though. I use the Möbius tool (Clark et al., 2001) to simulate the model and get the results. Theoretically, it would have been possible to model and solve it with a Markov model, but that had been very complex with that many states. I used the Markov model in *Paper G* where there is only one failure. That way, I got analytical results and did not need to use SAN and simulation.

## 1.6 Included Papers

The following papers have been produced during the PhD study period and aim to answer the listed research questions. These papers are included as Part II in this thesis. Note that some of the papers may have been subject to minor editorial changes since their publications.

- Paper A:  
**Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability**

Jonas Wäfler and Poul E. Heegaard

In Thomas Bauschert (Ed.), *Lecture Notes in Computer Science: Vol. 8115. Advances in Communication Networking* (pp. 185-196), Springer, 2013

This paper discusses the interactions between power grid and ICT components on a high level and serves as a common foundation for the other papers. We start bottom-up with the components constituting the smart grid and give a categorization based on their use of ICT. We then give state machines for the components and services and explain their interactions from a dependability perspective. Further, we discuss the positive and negative effects ICT can have on the dependability of the system. Finally, we introduce a meta-model which incorporates the information about the states of the components and services to create a state estimator for the smart grid considering ICT and power components.

- Paper B:  
**A Combined Structural and Dynamic Modelling Approach for Dependability Analysis in Smart Grid**  
 Jonas Wäfler and Poul E. Heegaard  
*Proc. 28th ACM Symposium on Applied Computing (SAC)*, Coimbra, Portugal, March 2013  

In this paper, we show how reliability block diagrams, pivotal decomposition and Markov models can be combined to exploit the complementary advantages of structural and dynamic models. In particular, we show how a Markov model can be used during the pivotal decomposition to include dependencies between entities, limited repair facilities, and other system dynamics in reliability block diagrams. This permits the qualitative and quantitative analysis of some classes of problems which are commonly solved only by simulation because the analytical solution is not feasible with the traditional models or are too complex. Further, we show how our approach can be used to assess the dependability in smart grids.
- Paper C:  
**Structural Dependability Analysis in Smart Grid under Simultaneous Failures**  
 Jonas Wäfler and Poul E. Heegaard  
*Proc. IEEE Smart Grid Communications (SmartGridComm)*, Vancouver, Canada, October 2013  

In this paper, we consider simultaneous failures in the network and explore how network percolation can be used for structural dependability analysis of the future power grid. We introduce new measures taking fundamental properties of the power grid into account, i.e. the connectivity between consuming nodes and power sources on the one hand and balancing the consumption and production in connected network components on the other. The measures are used in scenarios with random failures and intentional failures. The results are compared with the Largest Component measure and analyzed for their suitability for dependability and survivability analysis. Further, we show how to use these new measures to quantify the potential increase in dependability by using Demand Response and Distributed Energy Resources for the mitigation of the studied simultaneous failures.
- Paper D:  
**Quantifying Influence of Strategies and Network Properties in Repairing Simultaneous Failures in Smart Grid**  
 Jonas Wäfler and Poul E. Heegaard  
*Proc. Norsk Informatikkonferanse (NIK)*, Fredrikstad, Norway, Nov. 2014

In this paper, we continue the work from *Paper C* and analyze and compare several repair strategies to recover from simultaneous failures and quantify their performance during the repair time. In order to evaluate the different repair strategies we introduce a quantification method based on the accumulated cost of energy not delivered (CENS) during the repair. We consider the scenario in which the failure only affects the power grid and leaves the ICT system completely unaffected, i.e. the control center has the full information about the state of the whole network. We study how changes in the network, namely increasing the average node degree or increasing the number of power sources affect the repair costs. Further, we interpret our results in the advent of the smart grid services Demand Response and Distributed Energy Resources. And finally, we show how the results can be used for a survivability analysis.

- Paper E:  
**How to Use Mobile Communication in Critical Infrastructures: A Dependability Analysis**

Jonas Wäfler and Poul E. Heegaard

In Floor Koornneef, Coen van Gulijk (Eds.), *Lecture Notes in Computer Science: Vol. 9338. Computer Safety, Reliability, and Security*, Springer, 2015

In this paper, we suggest several alternatives on how a power utility may use mobile communication; we single out the four main future challenges and analyze how the alternatives are influenced by them. After this qualitative analysis we analyze the availability of the alternatives quantitatively based on measurement data from a Norwegian study. And finally, we analyze the availability improvement when equipping the base stations in the mobile network with more battery capacity.

- Paper F:  
**Interdependency in Smart Grid Recovery**

Jonas Wäfler and Poul E. Heegaard

*Proc. 7th International Workshop on Reliable Networks Design and Modeling (RNDM)*, Munich, Germany, Oct. 2015

In this paper, we focus on the interdependency between the power grid and the supporting ICT systems during the recovery process. We take a survivability approach in which the study starts the moment the system fails and ends with its full recovery. The recovery process is split into several phases and the interdependencies between power grid and ICT systems are analyzed step-wise for all of them. Based on this, we propose an analytical model for the recovery phase. First, it is used to investigate the potential of

automation and additional battery supply in the communication network to delay the interdependency effects between the systems. Second, it is used to analyze scenarios with different degrees of battery support, automation and number of repair crews, under high, medium and low frequency incidents. Finally, we discuss the impact of automation on the needed skill set for the repair crews and its implications for the recovery time.

- Paper G:

#### **Managed Dependability in Interacting Systems**

Poul E. Heegaard, Bjarne E. Helvik, Gianfranco Nencioni, Jonas Wäfler  
In Lance Fiondella, Antonio Puliafito (Eds.), *Principles of Performance and Reliability Modeling and Evaluation*. Springer, to be published in 2016

In this chapter, we address the dependability challenges related to complex system of systems. We discuss how adding automation in critical infrastructure influences the risks both with respect to the consequences and the probabilities. In order to increase the insight, a dependability modeling approach is taken, where the goal is to combine and extend the existing modeling approaches in a novel way. The objective is to quantify different strategies for management of dependability in interacting systems. Two comprehensive system examples are used to illustrate the approach. For this thesis only the second example is relevant. It builds loosely on paper F and demonstrates and discusses the consequences of adding more functionality to a smart grid, both in the distributed entities serving the primary function, and centralized in the control centre.

## **1.7 Thesis Structure**

The thesis is structured in two parts. Part I contains four chapters, including this one that motivates the thesis and gives the research questions. Chapter 2 presents the state of the art, Chapter 3 describes the contributions and discusses them and Chapter 4 contains concluding remarks and thoughts about future research directions. Part II provides the included papers. The appendix contains explanations for the formulas used in *Paper G*. I have chosen to include the papers in the same template as they were originally published. This results in a better recognition effect for readers having read the papers previously.





---

## State of the Art

In each of the included papers there is a section about the relevant related work for that specific study. In this chapter, I give an aggregated overview over the state of the art for the whole thesis. It is structured in two main parts: *challenges and modeling* and *analysis*.

### 2.1 Challenges and Modeling

The last years have seen an increase in research in complex systems. Several authors stress that when a system becomes more complex, the failures do not only increase linearly with the size but rather, systemic risks are increased. Helbing (2013) notes that “*complex systems have additional problems*” caused by their interdependencies. He adds that protection measures are not implemented because of “*insufficient theoretical understanding and, consequently, wrong policy decisions*”. Little (2002) looks at critical systems in general and notes that “*many problems will occur simply due to the complexity of these systems*” and Amin (2000) notes that “*conventional mathematical methodologies that underpin today’s modeling, simulation, and control paradigm are unable to handle their complexity and interconnectedness*”. These papers discuss the matter on a high level, and conclude that the challenges of complex systems lie in the different behavior of these systems and that a thorough analysis is crucial to prepare for the future challenges. They also state the problem that current models do not include these interdependencies; for the analysis they either have to be created from scratch or existing models need to be adapted.

#### 2.1.1 Modeling Complex System

The power grid, and even stronger the smart grid, is an instance of a complex system. However, the dependability and reliability analysis of power grids has traditionally not included the state of supporting ICT infrastructure (Bose, 2010;

Kirschen & Bouffard, 2009; Singh & Sprintson, 2010) and thereby ignored the influence the interdependencies between systems can have. Kirschen & Bouffard (2009) present an interdependency model for the power grid that illustrates how ICT and the power grid influence each other. In this model, depicted in Figure 2.1, both ICT and power grid have a binary state variable and can either be in a normal or abnormal state leading to a four-state model. It illustrates that, in addition to the traditional failure paths, the power grid can also fail as a consequence of an ICT failure. Being in the *Informationally Abnormal State* the failure probability for the power grid is different than in the *Normal State*. If the state of the ICT system is not considered, then this is ignored. In the paper they also give a list of past incidents, where the interdependency played a role. The model is very conceptual but can illustrate the main challenges.

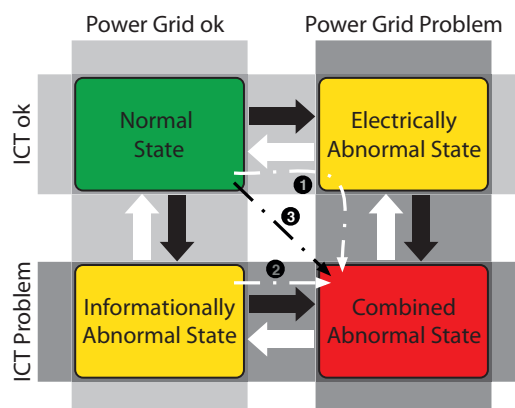


Figure 2.1: Four-state model showing the interdependency between ICT and power grid (based on model from Kirschen & Bouffard (2009)). The transitions marked with ①, ② and ③ represent a cascading, escalating and common cause failure, respectively.

A classification of particular types of failures which are caused by the interdependency of systems is put forward by Rinaldi et al. (2001). Failures are classified as *cascading*, *escalating* and *common cause* failures depending on the interaction of the systems. A *cascading failure* is defined as a failure in one system that causes an undesired event or failure in another system. An *escalating failure* is when an existing failure in one system escalates an independent failure in another system. And a *common cause failure* is a simultaneous failure in several systems caused by an external event or a failure of a shared resource or service. Figure 2.1 shows possible transitions of these failures in the four-state model. The transition marked with ① is an example of a *cascading failure*, a failure in the power grid

that leads to a failure in the ICT system. This could be a power outage, the ICT system is not provided with power anymore and stops working. The transition ② is an example of an *escalating failure*. In this case the ICT system was in the abnormal state, i.e. not working properly when an independent power grid failure happened. The latter failure is escalated by the failure in the ICT system. An example for that is a configuration error in a control system. When an independent power failure happens, the control system may react in the wrong way because of the error and escalate the already existing failure even more. The transition ③ is a *common cause failure*, for example caused by a storm affecting both the power grid and ICT infrastructure at the same time.

These three failure types are specific to interdependent systems and do not exist in simple systems. They are important causes for the additional challenges in the smart grid. Rinaldi et al. (2001) present in total six different dimensions for describing infrastructure dependencies. Another dimension that is worth mentioning is the dimension labeled as *Coupling and Response Behaviour*. It describes how tight or loose and how linear or complex the coupling is. This is an important point as the dependencies are often loose and complex, meaning a failure in one system leads only sometimes to a failure in the dependent system and the interaction is not always understood that well. The study presents a formal system for defining dependencies and is written in a way that fits various systems. This means it can be applied in many different domains such as transportation systems, agriculture and of course the power system. It leaves the investigator with the task of studying how these interdependencies manifest in a specific system.

The discussion of the three failure types in the four-state model shows also the limitations of the model. While it allows to demonstrate the interdependencies, it cannot be used for more detailed analysis. There are many more abnormal states in both systems with very different consequences, in an analysis they have to be differentiated. Other effects such as a back-and-forth cascading chain cannot be illustrated with the model.

Some of these problems are addressed by Laprie et al. (2007) presenting a model including the three above mentioned interdependency failures. They discuss in some details the interactions and create a model in which both systems have four to five different states. The model contains interesting features such as passive and active latent errors. Passive latent errors in a system are characterized by a passive malfunction, i.e. the system is not working when needed. Active latent errors lead to undesired actions such as execution of an action without having received a command. Both are latent errors that reside in a system until they provoke a failure, during this latent phase they might remain unnoticed by the control center for a long time. Latent errors, sometimes also just called errors (Avizienis et al., 2004), also exist in power grids, but ICT systems are more prone to such errors because of additional complexity due to their software components. There-

fore, these errors are instances of arising challenges brought by the increased use of ICT. In fact, Rahman et al. (2009) studied critical infrastructures in the US and came to the conclusion that more than 65% of all reported failures were software related, including software design, implementation, configuration, malicious logic fault inserted by an attacker, and authorization violation based on a faulty access control. These might be originating from a latent error. The model in Laprie et al. (2007) can be seen as an extension to the four-state model of Kirschen & Bouffard (2009), where the additional states allow a more detailed description of the system state. Its strengths lie in the inclusion of the new interdependency effects and the latent errors. It is still very high-level and the focus is mainly on the failing process, the repair process is not covered in the same level of detail. An example for that is the restoration of a power grid failure caused by a latent error, it is assumed that the next state is the state in which both systems are completely repaired, however, errors in the ICT system may be very hard to fix if they concern for example software bugs or faulty configurations.

A different way of extending the four-state model was chosen by Panteli et al. (2013). Their focus lies on the situational awareness, i.e. the potential discrepancy between the monitored state and the actual state of the system. The model they use duplicates all the states in the four-state model and adds the awareness information to the states. This addresses an important issue, which was partially addressed in Laprie et al. (2007) with the latent states, but it does not significantly extend the way the model can be used. The models have in common, that they describe some of the future challenges on a high level and they are meant to be used in a qualitative analysis.

A more practical approach is taken by Utne et al. (2011). They propose a method for assessing interdependencies of critical infrastructure, focusing on a step-wise process including both qualitative and quantitative analysis. After defining an initial event the steps identify interdependencies and perform quantitative and qualitative analysis. Their method works with cascading diagrams defining different consequences of the initial event. Kjølle et al. (2012) shows a variation of this approach and gives a case study in an emergency preparedness context. Both studies focus on risk analysis, the concrete models used to get a quantitative result are not specified or are based on power flow and dependability analysis of power systems, respectively.

### **2.1.2 Network Robustness**

Research in network robustness has seen a lot of activity in the past years. Studies include various networks including the internet (Albert et al., 2000; Cohen et al., 2000) but also the power grids (Albert et al., 2004; Solé et al., 2008; Wang et al., 2010b). These studies model the simultaneous failure based on percolation theory

which describes the behavior of the size of the largest connected network component after the removal of a fraction of  $1 - p$  of the  $n$  nodes of a network. A network component is a part of the whole network in which any two nodes are connected with a path and which is not connected to other nodes from the network. If a critical fraction of nodes  $1 - p_c$  is removed, the largest component collapses for a high number of nodes. The percolation point  $p_c$  and the size of the largest component after a failure of a fraction of  $1 - p$  nodes are used as indicators for the structural vulnerability or robustness. The latter is called *Largest Component* measure and  $p$  uses usually the whole range from 0 to 1.

In Albert et al. (2004) an additional measure is defined, which takes connections between consumers and power sources into account. The number of power sources reachable from each node is counted before and after the incident and the averaged difference is then called *connectivity loss*. This measure yields less theoretic results as the *Largest Component* measure, however, it measures only the change and gives no indication about the absolute number of disconnected nodes after the incident.

Several previous studies stress the importance of adapting purely topological measures to the specific needs of the power grid and extend centrality measures with electrical parameters such as impedance (Wang et al., 2010a), impedance and power flow (Arianos et al., 2009), electrical distance, power transfer distribution and line flow limits (Bompart et al., 2012). They have in common, that they analyze the relative importance of nodes and lines with the aim to find vulnerable parts of the system.

The study of Buldyrev et al. (2010) goes one step further: Here the authors include the interdependencies between the power grid and the supporting ICT network in their model. Both networks are represented as a graph and the mutual dependencies are modeled as an additional type of link connecting the two networks. A failure of a node leads directly to a failure of all dependent nodes, i.e. they assume a tight coupling between the systems. Their model is based on a cascading failure that goes back-and-forth between the two systems until it reaches a steady state. They explicitly note the smart grid and a major outage in the past as a motivation for their model.

All the studies have in common, that they work on a very high abstraction level and the details of the events stay unclear. The results give information about some properties of the network but the implications for a power grid are open.

## 2.2 Analysis

There are a couple of studies about past power grid incidents, which show that some of the proclaimed future challenges in the smart grid already exist to a cer-

tain extent in the current power grid (Andersson et al., 2005; Buldyrev et al., 2010; Kirschen & Bouffard, 2009; Xie et al., 2002). A chain of cascading failures, i.e. failures in one system that trigger failures in another system, was a major reason for the large blackout in Italy in 2003 (Buldyrev et al., 2010). An escalating failure, i.e. independent failures in systems that amplify each other, was an important reason why the blackout in the US in 2003 could become so large (Andersson et al., 2005). The analysis of disturbances in the US power grid from 1979 to 1995, to which I have already referred to in the introduction, finds that problems in ICT related systems like monitoring and communication systems “*contribute to a very high percentage of large failures*” (Xie et al., 2002). Kirschen & Bouffard (2009) cite more examples in which ICT systems caused or escalated a failure in the power grid.

ICT will play a bigger role in the smart grid and the control centers have to include the state of it in their system state. Line (2015) studied how well power utilities are prepared to handle ICT incidents and found that the risks are often not addressed well, partly because of a different understanding of the challenges and different priorities among business managers, IT and control personal. The study is limited to information security incidents, but the gap between the ICT and power personal might be similar when looking at ICT dependability incidents.

Bae & Thorp (1999) use a rare event technique to model and analyze a power system to find weak links. The study analyzes latent errors in the protection system, which consists of relays throughout the system and is responsible to protect the system from damage. Each relay has a small controller deciding on its own if the relay should be opened or not. False operation by the controller can either lead to damage in the system, if the controller does not open the relay in time or to additional outages, if the tripping was not necessary. Latent errors, or hidden failures as they are referred to in this study, are made responsible for escalating power grid failures in two major outages in 1996.

### 2.2.1 Structural Analysis

In Solé et al. (2008) the relation of the percolation point  $p_c$  of 19 european transmission grids is investigated to non-topological dependability measures such as average interruption time, power loss and energy not delivered. Dividing the grids into two groups based on their node degree distribution, the authors find a correlation between this grouping and the empirical dependability indices.

Wang et al. (2010b) study the percolation point in american power grids and on IEEE model systems. The study is done for both random and selective node break down. Using the *Largest Component* measure they find that selective node breakdowns have a much higher effect on the robustness of the system than random node breakdown.

However, it is not clear yet how to use these results for a dependability analysis as this *Largest Component* measure and its percolation point is agnostic to characteristics of the underlying network.

### 2.2.2 Cascading Failures

There are several studies analyzing the behavior of interdependent networks on a structural level. Buldyrev et al. (2010) create a model of two interdependent networks and study their behavior when removing nodes, i.e. inspired by percolation theory as explained above. They analyze simple networks and interdependent networks and find that the behavior of networks changes when introducing interdependency. In a follow up study Parshani et al. (2011) show that increasing the number of interconnections and thereby increasing the interdependency between the systems, leads to a higher vulnerability to random failures. While interesting on a theoretic level, there is no information about the details causing the cascading steps and hence, it is not clear if such a scenario is realistic at all. In addition, the authors use the largest component measure, which gives in my opinion very limited information about the state of a network.

A similar approach is taken by Svendsen & Wolthusen (2007), the networks are chosen in a way to match the topologies of the power grid and the telephony network. The power devices rely on information from the telephony system and the telephony system relies on power supply from the power grid; a failure of any node leads to a failure of all dependent nodes. The analysis contains information about how the power grid and the telephony network react on single and multiple failures in the power grid. This is done once for a one-way dependency of the telephony network on the power grid and once for a two-way dependency, i.e. interdependency. Their results show that the interdependency has a very strong effect on both networks. Even though this study goes into some details such as the different topologies and models the interactions between the system nicely, they fail to motivate why a node in the power grid is disconnected from the grid if no information is available. Only this tight dependency between the ICT system and the power grid allows the devastating effect of cascading failures as shown by them and the two studies mentioned above.

Morris & Barthelemy (2013) also model the power grid as two networks, the power grid itself and a control network covering parts of the power grid. A propagating failure is modeled by an initial failure that leads to a load redistribution in the power grid. If the load on a line rises over the maximum capacity, the control node in an adjacent substation tries to dissipate the excess power and thereby avoid an overload failure. If it is not successful, the line fails and loads are redistributed in the system, which may lead to a propagation of failures in the system. The failure is not defined in more details, it could be a latent error, i.e. the system



is not performing as it should, or simply a situation in which it is not possible to dissipate the excess power. The cascading failure is then given by power outages resulting in unpowered control devices and control devices not managing to stop the overloaded situation.

### 2.2.3 Adding New Services

According to European Commission (2006) one of the objectives of the smart grid is to improve the dependability of the power grid with the help of new services supported by ICT systems. Vadlamudi et al. (2014) analyze 10 smart grid technologies for their potential dependability contribution. The qualitative analysis yields for all technologies a reduction of either the *frequency* of failure events, the *duration* of failure events, or both. The improvement comes from, among others, additional power generators throughout the network, load control and more monitoring devices to increase the situational awareness. These technologies rely heavily on a working and reliable ICT system. Faulty ICT support is not considered in this study.

Strbac (2008) analyzes the benefits and challenges of demand response (DR), which is a technology for adjusting the load dynamically depending on the grid state and is either locally or remotely controlled. He sees benefits for the dependability by using DR to reduce the load in case of a power shortage caused by an outage in the grid and thereby mitigate the outage temporarily. As a challenge he notes that the additional ICT systems “*increase the complexity of the system operation when compared with traditional solutions*”. The challenge is the reliable operation of this complex system.

The risks are clearly underlined by NERC (NERC Report, 2010). In their report they discuss dependability challenges that arise with the introduction of new technology. They issue the following warning statement as one of their conclusions: “*While the promise of smart grid is, in part, to enhance reliability, if it is poorly deployed the reliability of the bulk power system could suffer. Therefore, it is vitally important to ensure the evolution of smart grid does not increase the bulk power system’s vulnerability, but rather supports industry’s bulk power system reliability goals.*”. The report does not contain analysis but gives recommendations on how to proceed. It includes creating new models taking the interdependency between power and ICT systems into account; which is the aim of this thesis.

---

## Contribution and Discussion

In this chapter, I first give the contributions to the research questions, followed by the discussion and the implications for the power utilities.

### 3.1 Contribution

Figure 3.1 gives an overview over the papers, their relevance to the research questions, their direct implications on the overall objective and how they relate to each other.

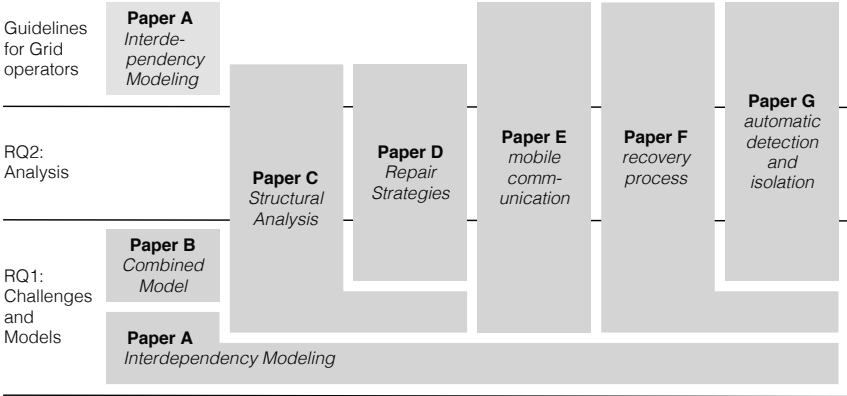


Figure 3.1: Overview over the included papers.

Table 3.1: Dependencies considered in the papers.

Paper	Failure Chain		Details
	ICT →PG	PG →ICT	
<i>Paper A</i>	X	X	cascading and escalating failures between PG and ICT
<i>Paper B</i>	(x)	(x)	models could be used for both
<i>Paper C</i>	X		new failure patterns in PG due to cascading effect from ICT
<i>Paper D</i>	X		new failure patterns in PG due to cascading effect from ICT
<i>Paper E</i>		X	cascading failure from PG to ICT, plus common cause failures between mobile networks
<i>Paper F</i>	X	X	cascading failure from PG to ICT, escalating failure from ICT to PG
<i>Paper G</i>	X	X	cascading failure from PG to ICT, escalating failure from ICT to PG

### 3.1.1 Contribution to RQ1: Challenges and Models

The contributed papers show how the transition towards a smart grid increases the interdependencies between the power grid and the supporting ICT systems. Additionally, they illustrate and discuss how some of these interdependencies look like in more detail than previously studied and what the resulting challenges are. Table 3.1 gives an overview of the covered dependencies in the papers.

The thesis identifies the following future challenges: cascading, escalating and common cause failures, higher possibility for simultaneous failures caused by a cascading failure from the ICT system, passive and active latent errors, and the risks of automation. They have all been mentioned in the literature before, the contribution of this thesis is to give concrete examples and investigating them in more detail including giving use cases with models and then analysing the implications of them.

*Paper A* explains on a component level how a failure can cascade or escalate from the power grid to the ICT system, and vice versa. It shows that the system can fail in new ways because new interdependencies are introduced in the smart grid, which create new types and patterns of faults and failures, specifically: cascading and escalating failures, and latent and passive errors. The paper presents a way how to model smart grid entities. The resulting challenge is to recognize the interdependencies in a given system and create a large model. The paper also discusses techniques and models for the quantitative analysis, but only on a high

level as this has to be chosen depending on the specific use case. The proposed meta-model is supposed to be used primarily as a condensed state visualization or for the incident analysis.

*Paper B* is purely concerned about the use of structural and dynamic models. Its contribution to RQ1 is the discussion of combination of modeling techniques to solve some typical issues encountered when using reliability block diagrams.

The remaining papers address specific use cases. Their main contributions to RQ1 lie in the description of threats, their manifestation and the modeling part. The first use case is based on a cascading failure from the ICT system to the power grid. A simultaneous failure in several ICT nodes cascades to the power grid and creates there a simultaneous failure, thereby increasing the frequency of this type of failure and changing the failure pattern in the power grid. This use case is the starting point for both *Paper C* and *Paper D*. The modeling and especially the new measures are the main contribution to RQ1 from these papers.

*Paper E* focuses on a cascading failure from the power grid to an ICT system, namely a mobile communication system. Its contributions are, first, the discussion of primary challenges in mobile communication, which a power grid operator has to consider. And second, the models for the common cause failure in the mobile networks and the models including battery support for temporary failure mitigation.

The use case for *Paper F* and *Paper G* is based on the recovery process in smart grids. Part of the contribution here is the process itself, which has an interesting interdependency with cascading and escalating failures. The main contribution for RQ1, however, is the modeling of failures in the supporting ICT systems and the risk curve method to visualize and analyze the change of risks when increasing the automation of processes.

### **3.1.2 Contribution to RQ2: Impact Analysis**

*Paper A* analysis the interaction between smart grid components in a qualitative way. For each state a component can be in, its implication on other components is analyzed. In addition, it is discussed passive and active latent errors can lead to a divergence of the perception and the actual state of components.

*Paper C* analyzes the impact of a simultaneous failure in a typical Norwegian power grid. It is a purely structural analysis and its contributions to RQ2 are: First, showing that the network topology and the placements of power plants therein influences the dependability. As a consequence, the chosen dependability measure is crucial to assess the state of the system in a detailed enough way. Second, discussing the very different behavior of the system when changing from random failures to intentional failures, i.e. deliberate attack on the most crucial parts in the network. And third, the quantitative discussion of how much the smart grid

services demand response, distributed energy resources or micro grid may potentially improve the dependability in this context.

*Paper D* focuses on the performance of repair strategies after a simultaneous failure. Its main contribution to RQ2 is to show how to select the optimal next node to repair and that the strategy of choosing this next node has a large impact on the performance and total costs of an outage. The performance depends strongly on the network topology and network properties such as number of power grids. An additional contribution is like in *Paper C* the quantitative discussion on the improvements potentially achievable with the smart grid services demand response, distributed energy resources or micro grid.

*Paper E* discusses mobile communication as an option for the communication layer for parts of the power grid. Its contributions are the different alternatives of how to use mobile communication and how they face the primary future challenges. Additionally, the availability of all the alternatives are computed based on Norwegian measurement data. The final contribution is the analysis of how the availability changes when the cascading failure in the mobile network is temporarily mitigated by a limited battery support.

*Paper F* describes a use case in which a failure not only cascades from one system to the other, but also comes back to the original system. Its fundamental contribution is the illustration of a back and forth cascading and escalating failure in a real system and the discussion of ICT dependency for each phase and step of the power grid recovery process. Additionally, it analyzes the availability increase by adding an automatic detection and battery support in the supporting communication system. Its main contribution, however, is the quantification and discussion of the changing consequences for high and low frequency failures due to automation and its impact on the role of the repair crews.

The contribution of *Paper G* for RQ2 is that it puts the potential change of risks of system due to automation in a bigger context. Additionally, the included smart grid example discusses the interdependencies during the first stage of the recovery process of the power grid in more details. Its contribution is to discuss how the introduction of automation reduces the down time per outage but increases the frequencies of outages, because of malfunctioning ICT. Further, it shows how the malfunctioning ICT system can partly negate the positive effect of its introduction.

## 3.2 Discussion

In the following the implications and limitations of the thesis contributions are discussed. The discussion follows the structure of the two major research questions and is then completed by implications and guidelines for grid operators.

### 3.2.1 Discussion of RQ1: Challenges and Models

The new challenges increase the complexity of the system, which in turn can lead to even more failures. A study by Norros et al. (2012) discusses that complexity in systems is a strong driver for human errors, which constitutes the biggest error type in certain systems (Kuhn, 1997). *Paper A* can be seen as an introductory paper describing most of these challenges. It describes the interdependencies on a component level. I present models for all of the challenges. However, models always depend strongly on the objective of the study and have to be adjusted for other studies.

My model in *Paper A* allows modeling software errors that are difficult to detect and remove, because the removal of a failure does not necessarily mean the removal of an error (Avizienis et al., 2004). This is not covered in the model presented by Laprie et al. (2007). However, the model is only given for components and not for a larger system. The meta-model also presented in *Paper A* extends the model from Kirschen & Bouffard (2009) and allows to model passive and active latent errors. ICT components are more complex than common power grid components because of the complexity in the software. Therefore, the concept of errors is important. In general it has a similar application as the four-state model in Kirschen & Bouffard (2009) but suffers also the same drawbacks, i.e. longer back-and-forth cascading chains cannot be modeled and it hides a lot of information. I believe that it can be very useful for situational awareness and in qualitative analysis especially when supplemented with information about the individual steps as shown in *Paper A* and in *Paper F*.

As a next step, I use a top-down approach to model a simultaneous failure in a power grid, focusing purely on the structural dependability. The proposed measure extends the biggest component measure used in many studies such as Solé et al. (2008) and Buldyrev et al. (2010) and thereby yields more relevant information about the robustness of a power grid. This is discussed in more details in *Paper C* and to some degree in *Paper D*. However, it still stays on a high abstraction level and it gives only a limited view of the grid, but it can be interpreted as the best case scenario in case of an incident, i.e. when all the other challenges are met. I choose to work with node failures in the network and do not consider link failures. This corresponds to the usage in literature. The main reason for me to use node failures was that statistics from the Norwegian power grid shows that failures in the substation are more frequent than link failures (ENTSO-E, 2010). This varies strongly between different countries and it has to be noted that the failures in the substation usually do not affect the whole substation but only one part. The assumed node failures are therefore not that frequent. I did analysis with link failures and the results were similar, however, there is a looser coupling between link failures and power outages as there are usually alternative routes available.

The probability of such a simultaneous failure is difficult to quantify. In the literature the increasing failure is used primarily to assess the robustness of the structure in a theoretic way and not that much to compute the risk of the failure. However, there is a certain probability that a simultaneous failure may happen and it is increasing in the smart grid. In *Paper C* and *Paper D*, I give a motivation for this failure, although it is unlikely that it affects a large number of nodes.

In the last two papers I focus not on the structure but on a process. The inspiration comes from other studies that use cascading chains between the power grid and the ICT system (Buldyrev et al., 2010; Parshani et al., 2011; Svendsen & Wolthusen, 2007). The coupling used in these studies is very tight and not explained in details. It is not clear why and how these back-and-forth cascading work in detail. In *Paper F*, I give a specific example on how a power grid failure cascades to a part of the ICT system and how this in turn escalates the failure in the power grid. The cascading chain stops after two steps. It would be interesting to find a realistic longer chain, but it is difficult to do that without introducing too many assumptions. Assuming a power grid component to fail or stop working when an ICT component is not working seems to be a very strong assumption. Utility personal I talked to say that in the current power grid this is highly unlikely, as the power grid can run blindly for a certain time period. But it is probably possible to construct a case with future technology or services where the dependency is higher. The most realistic example of a failure chain is presented in Morris & Barthelemy (2013). Although, strictly speaking it is mainly a propagating overload failure inside the power grid, which the control system tries to stop. It is not a classical back-and-forth cascading chain as assumed in the papers above.

### 3.2.2 Discussion of RQ2: Impact Analysis

The qualitative and quantitative analysis of cascading and escalating failures shows that the risks outlined in Kirschen & Bouffard (2009) are realistic and have a strong impact on dependability. The different analyses are done for specific use cases and it remains unclear what the overall impact would be. The advantage of use cases is that they are more concrete and utilities can relate to them.

The analysis of the structural dependability in *Paper C* and *Paper D* shows how important it is to include topology in the analysis. If the topology is not included, the effect of a failure is assessed to be lower than when including the topological effect. Additionally, when repairing a system, the knowledge about the topology can reduce the consequences of an outage. The measures play also an important role. There are many more measures, like for example various centrality measures that are compared in Wang et al. (2010a). The choice depends on the objective of the study and there is no single best measure. The analysis also shows that future smart grid technologies and concepts such as demand response,

distributed energy resources and micro grids may have a strong impact on the dependability of the system. In *Paper C* and *Paper D*, I quantify this improvement, which was proclaimed in Vadlamudi et al. (2014). However, in these examples, I do not consider a malfunctioning of the new technologies. Passive latent failures may reduce some of the improvement and active latent failures may even have a negative effect, as explained in *Paper A* and *Paper G*. I did not conduct the analysis with faulty ICT systems because the focus of these studies was primarily on the simultaneous failure and in a second step on the potential of new technologies to improve the dependability. It assumes a best-case scenario in order to show the possible potential.

The analysis results depend strongly on the input data, this is especially true for the study on mobile networks in *Paper E*. I build on the data from Kvalbein (2013). The two mobile operators from that study have very different up and down times. One has many failures that are short and in total a low unavailability and the other has fewer failures with much longer downtimes resulting in a higher unavailability. These properties guide the recommendations about when to utilize the different usage alternatives. When considering different operators, these recommendations will be different. However, the usage alternatives and the models are still valid.

Introducing new technologies may not only bring advantages but may also have negative consequences as stated in Heller (2001). My two studies analyzing the power grid restoration process quantified this effect. Working with rare events is difficult as they, by nature, are not happening that often. I chose to use the survivability approach as explained in Heegaard & Trivedi (2009), in which the rare events do not need to be estimated, only the consequences are analyzed, i.e. the system behavior immediately after a failure is quantified. In *Paper F* I give some rough estimate about how often such an event may happen. The aim of this study is not to get a correct numerical estimate, but to show that such events indeed exist. In case of the rare events I had to make assumptions about the reduction of repair crews and the change of repair rates due to missing training and practice. Those are partly educated guesses. But from the results it can be seen, that changing the parameters changes the amplitude but not the conclusion.

### **3.2.3 Implications and Guidelines for Grid Operators**

The contributions to RQ1 and RQ2 indicate that the new challenges have the potential to both negatively and positively influence the dependability of the smart grid. What are the implications for the grid operators and how can they address these issues? In the following I list the most important guidelines implied by the contributions, together with a short discussion. In parentheses I indicate from which paper the contribution is coming from.



### **Create awareness: Be aware of interdependencies and the new failures and failure patterns**

The most important message for grid operators is to understand that the smart grid has an increased interdependency between the power grid and the ICT system. Creating awareness for this is of utter importance. All papers address this issue. A meta-model (*Paper A*) may be useful to visualize the interdependencies. Different failure patterns may emerge because of cascading failures from another system, like for example a higher frequency of simultaneous failures (*Paper C, Paper D*). The smart grid is also more susceptible to directed attacks, while this is not the focus of this thesis, it is worth noting that the impact of a directed attack is much more severe than random failures (*Paper C*). Failures may be escalated because of a failure in a dependent system (*Paper A, Paper F and Paper G*).

### **Automation: Be aware of malfunctioning ICT**

It might be obvious, but ICT can and will fail at some point. Therefore, it is important to investigate the effects of a malfunctioning ICT system whenever a new ICT system is added or a step is automated. Automation may lead to a shorter down time but at the same time to a higher frequency of failures as there are more components that can fail (*Paper G*). The automation may give a higher availability and lower consequences of frequent failures but it may lead at the same time to more catastrophic failures in rare events as both more components and more powerful components are involved. Automation has, therefore, to be accompanied by a careful analysis and additional preparedness measures (*Paper F and Paper G*).

### **Modeling: Inclusion of interdependency in dependability model**

From the analysis it follows, that it is crucial to include the state of both the power grid and the ICT system in the dependability analysis (*Paper A, Paper B, Paper F and Paper G*).

### **System analysis: Understand your system and their interdependencies**

For a grid operator it is important to know their systems and understand where the interdependencies lie and how they can manifest. Structural analysis can give important information about the structural dependability of a network (*Paper C and Paper D*). The system also relies on external services such as mobile communication (*Paper E and Paper F*). And it is important to analyze interdependencies in processes, e.g. the recovery process (*Paper F and Paper G*). There are many more interdependencies that are sometimes difficult to discover, e.g. the dependency between different mobile networks (*Paper E*).

**Preparedness: Be prepared for new failures**

The knowledge about the system and its properties can be used to increase the preparedness. Having the right processes and enough trained people for the incidents is crucial. This is even more important for failures in automated systems as the personal usually relies on support from the system, which might be down, and failures are potentially more complex (*Paper F* and *Paper G*). Repair strategies should be evaluated and chosen beforehand based on the system properties (*Paper D*).

**Mitigation: Mitigate a failure that cannot be prevented**

If a failure cannot be prevented, it might be mitigated. New smart grid services such as demand response, distributed energy resources and micro grid might have a great potential helping to mitigate the impact of a failure (*Paper C* and *Paper D*). In interdependent systems it might also be possible to temporarily prevent the interdependency failure by some means, e.g. installed battery support can allow to use the communication network for a certain time even without power supply from the grid (*Paper F*). Shortening the downtime might prevent the further cascading or escalation of a failure. The shortening can be achieved by technical means (*Paper F*) or by preparedness as discussed above and involves defining good processes and the right training for the responsible people.



---

## Concluding Remarks

Properties of the power grid vary strongly between countries and with that the focus in the smart grid is certainly very different. However, the challenges listed here should concern all of them because they are based on the increasing use of ICT.

In my opinion, the most important part is to create awareness about the future challenges. I believe that easy understandable models like the one presented in this thesis (*Paper A*) or from Kirschen & Bouffard (2009) can help to illustrate the risks to a broader audience. It remains then a matter of taste to choose a model. The model from Laprie et al. (2007) for example, includes more information, but in my opinion it is more difficult to grasp than the meta-model I presented in *Paper A*. the latter can also be extended by duplicating it and using one to indicate the actual system state and the other the state as perceived by the control system. This allows to explain the problem of state awareness. The risk curve figure used in *Paper F* and *Paper G* is another example that can be used to talk about the risks on a easy understandable level.

Another good option is to create use cases, which explain step by step how interdependent systems affect each other and create situations and failures that are new or more frequent than without the dependencies. *Paper F* and *Paper G* do exactly that but of course there are many more.

An important step is to convince the decision makers about the problem and get their attention for this topic. An alternative route is via the regulator that could oblige utilities to assess the system for the future challenges. It is also crucial that international bodies discuss the risks of the extension of smart grids like it is done by NERC (NERC Report, 2010).

There are several interesting directions for future research, I am presenting here the two that are most intriguing to me. The liberalization of the electricity market and the partial outsourcing of services, e.g. support or operation of ICT systems, have created new interdependencies. In both cases, the number of actors increases and with that raises the complexity of the system. Business processes

are spread across several organizations and companies, which leads to new challenges. Line (2015) notes for example, that some power utilities seem to rely almost blindly on ICT contractors to handle possible information security incidents. This is especially true for smaller utilities, which might lack the resources and the knowledge to operate their ICT systems in-house. Responsibilities might not be defined clearly enough, particularly in cases of emergency. The level of preparedness may differ significantly between the different parties and affect the consequences of an outage. A good starting point for the dependability consequences of the liberalization of the electricity market is the article by Antonsen et al. (2010).

Another relevant topic for the future, which I only briefly touched upon, is how the knowledge about the system and the usage of new technologies can be used to minimize the effect of unavoidable failures, i.e. increase the systems survivability. Nobody can control blizzards or hurricanes, but operators can prepare themselves for it. One way is by conducting survivability analysis to find more robust working states in which the system can transition once a certain event is predicted. With modern smart grid technologies there are even more options. For example, demand response might be used to shift loads away from the predicted event time and geographical region, and micro grids could be prepared to switch to independent operation. This leads to less load during the predicted time period an event occurs and thereby the consequences of the event are reduced. A starting point for this is the work by Dikbiyik et al. (2014) on proactive disaster protection in optical backbone networks.

This thesis is a small step towards reliable smart grids; the field remains interesting and challenging, not least because the power grid has a central role in our society and at the same time high dependability requirements.

---

## References

- Albert, R., Albert, I., & Nakarado, G. L. (2004). Structural vulnerability of the north american power grid. *Physical Review E*, 69(2), 025103.
- Albert, R., Jeong, H., & Barabási, A.-L. (2000). Error and attack tolerance of complex networks. *Nature*, 406(6794), 378–382.
- Amin, M. (2000). National infrastructure as complex interactive networks. In T. Samad & J. Weyrauch (Eds.), *Automation, control and complexity* (pp. 263–286). New York, USA: Wiley.
- Andersson, G. et al. (2005). Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance. *IEEE Trans. Power Syst.*, 20(4), 1922–1928.
- Antonsen, S., Almklov, P. G., Fenstad, J., & Nybø, A. (2010). Reliability consequences of liberalization in the electricity sector: Existing research and remaining questions. *Journal of Contingencies and Crisis Management*, 18(4).
- Arianos, S., Bompard, E., Carbone, A., & Xue, F. (2009). Power grid vulnerability: A complex network approach. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 19(1), 013119–013119–6.
- Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable and Secure Computing*, 1(1), 11–33.
- Bae, K. & Thorp, J. S. (1999). A stochastic study of hidden failures in power system protection. *Decision Support Systems*, 24(3–4), 259–268.
- Bompard, E., Pons, E., & Wu, D. (2012). Extended topological metrics for the analysis of power grid vulnerability. *IEEE Systems Journal*, 6(3).

- Bose, A. (2010). Models and techniques for the reliability analysis of the smart grid. In *Proc. IEEE PES General Meeting, Minneapolis, USA* (pp. 1–5).
- Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, 464(7291), 1025–1028.
- Clark, G., Courtney, T., Daly, D., Deavours, D., Derisavi, S., Doyle, J. M., Sanders, W. H., & Webster, P. (2001). The möbius modeling tool. In *International Workshop on Petri Nets and Performance Models, Aachen, Germany*.
- Cohen, R., Erez, K., ben Avraham, D., & Havlin, S. (2000). Resilience of the internet to random breakdowns. *Physical Review Letters*, 85(21), 4626–4628.
- Dikbiyik, F., Tornatore, M., & Mukherjee, B. (2014). Minimizing the risk from disaster failures in optical backbone networks. *Journal of Lightwave Technology*, 32(18).
- EPRI (2015). <http://smartgrid.epri.com>. [online; accessed 16 Nov 2015].
- European Commission (2006). *European Smart Grids Technology Platform - Vision and Strategy for Europe's Electricity Networks of the Future*. Technical report.
- European Commission (2010). *European Smart Grids Technology Platform - Strategic deployment document for Europe's Electricity Networks of the Future*. Technical report.
- European Network of Transmission System Operators for Electricity (ENTSO-E) (2010). Nordic Grid Disturbance and Fault Statistics 2010. [https://www.entsoe.eu/fileadmin/user\\_upload/\\_library/publications/entsoe/RG\\_SOC\\_Nordic/110831\\_NORDIC\\_GRID\\_DISTURBANCE\\_AND\\_FAULT\\_STATISTICS\\_2010.pdf](https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/RG_SOC_Nordic/110831_NORDIC_GRID_DISTURBANCE_AND_FAULT_STATISTICS_2010.pdf).
- Følstad, E. L. & Helvik, B. E. (2011). Failures and changes in cellular access networks; a study of field data. In *Proc. DRCN* (pp. 132–139).
- Heegaard, P. E. & Trivedi, K. S. (2009). Network survivability modeling. *Computer Networks*, 53(8), 1215–1234.
- Helbing, D. (2013). Globally networked risks and how to respond. *Nature*, 497(7447), 51–59.
- Heller, M. (2001). Interdependencies in civil infrastructure systems. *The Bridge*, 31(4), 9–15.

- IEEE/CIGRE Joint Task Force on Stability Terms and Definitions (2004). Definition and classification of power system stability. *IEEE Trans. Power Syst.*, 19(3), 1387–1401.
- Kirschen, D. & Bouffard, F. (2009). Keeping the lights on and the information flowing. *IEEE Power and Energy Magazine*, 7(1), 50–60.
- Kjølle, G., Utne, I., & Gjerde, O. (2012). Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies. *Reliability Engineering & System Safety*, 105(0), 80–89.
- Kuhn, D. (1997). Sources of failure in the public switched telephone network. *Computer*, 30(4), 31–36.
- Kvalbein, A. (2013). *Robusthet i norske mobilnett*. Technical report, [Robustness in Norwegian mobile networks], simula research laboratory.
- Laprie, J.-C., Kanoun, K., & Kaâniche, M. (2007). Modelling interdependencies between the electricity and information infrastructures. In *Proc. SAFECOMP, Nuremberg, Germany* (pp. 54–67).
- Line, M. B. (2015). *Understanding information security incident management practices – A case study in the electric power industry*. PhD thesis, NTNU.
- Little, R. G. (2002). Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures. *Journal of Urban Technology*, 9(1), 109–123.
- Morris, R. G. & Barthelemy, M. (2013). Interdependent networks: the fragility of control. *Scientific Reports*, 3.
- National Energy Technology Laboratory (NETL) (2009). *A vision for the modern Grid*. Technical report, U.S. Department of Energy.
- National Energy Technology Laboratory (NETL) (2010). *Understanding the Benefits of Smart Grids*. Technical report, U.S. Department of Energy.
- NERC Report (2010). *reliability considerations from the integration of smart grid*. Technical report, NERC.
- Norros, L., Norros, I., Liinasuo, M., & Seppänen, K. (2012). Impact of human operators on communication network dependability. *Cognition, Technology & Work*, (pp. 1–10).



- Panteli, M., Crossley, P. A., Kirschen, D. S., & Sobajic, D. J. (2013). Assessing the impact of insufficient situation awareness on power system operation. *IEEE Transactions on Power Systems*, 28(3).
- Parshani, R., Buldyrev, S. V., & Havlin, S. (2011). Critical effect of dependency groups on the function of networks. *Proc. National Academy of Sciences of the United States of America*, 108(3), 1007–1010.
- Rahman, H. A., Beznosov, K., & Marti, J. R. (2009). Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. *Int. J. of Critical Infrastructures*, 5(3).
- Rinaldi, S., Peerenboom, J., & Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11–25.
- Rosas-Casals, M., Valverde, S., & Solé, R. V. (2007). Topological Vulnerability of the European Power Grid under Errors and Attacks. *Int. J. of Bifurcation and Chaos*, 17(07), 2465–2475.
- Sanders, W. H. & Meyer, J. F. (2001). Stochastic activity networks: Formal definitions and concepts. In *Lectures on Formal Methods and Performances Analysis*, volume 2090. Springer.
- Singh, C. & Sprintson, A. (2010). Reliability assurance of cyber-physical power systems. In *IEEE PES General Meeting, Minneapolis, USA* (pp. 1–6).
- Solé, R. V., Rosas-Casals, M., Corominas-Murtra, B., & Valverde, S. (2008). Robustness of the european power grids under intentional attack. *Physical Review E*, 77(2).
- Strbac, G. (2008). Demand side management: benefits and challenges. *Energy Policy*, 36(12), 4419–4426.
- Svendsen, N. K. & Wolthusen, S. D. (2007). Connectivity models of interdependency in mixed-type critical infrastructure networks. *Information Security Technical Report*, 12(1), 44–55.
- Utne, I., Hokstad, P., & Vatn, J. (2011). A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering and System Safety*, 96(6), 671–678.
- Vadlamudi, V. V., Karki, R., Kjølle, G. H., & Sand, K. (2014). Reliability-centric studies in smart grids: Adequacy and vulnerability considerations. In *Reliability Modeling and Analysis of Smart Power Systems*. Springer.

- Wang, Z., Scaglione, A., & Thomas, R. (2010a). Electrical centrality measures for electric power grid vulnerability analysis. In *Proc. IEEE Conf. on Decision and Control (CDC), Atlanta, GA*.
- Wang, Z., Scaglione, A., & Thomas, R. (2010b). The node degree distribution in power grid and its topology robustness under random and selective node removals. In *Proc IEEE Int. Conference on Communication (ICC), Cape Town, South Africa*.
- Wolfram Research (2012). Mathematica 9.0.1. <https://www.wolfram.com/mathematica/>.
- Xie, Z., Manimaran, G., Vittal, V., Phadke, A. G., & Centeno, V. (2002). An information architecture for future power systems and its reliability analysis. *IEEE Trans. Power Syst.*, 17(3), 857–863.



PART II

---

**INCLUDED PAPERS**



---

# Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability

Jonas Wäfler and Poul E. Heegaard

In Thomas Bauschert (Ed.), *Lecture Notes in Computer Science: Vol. 8115. Advances in Communication Networking* (pp. 185-196),  
Springer, 2013

© 2013, IFIP International Federation for Information Processing. Reprinted with permission.



# Interdependency Modeling in Smart Grid and the Influence of ICT on Dependability

Jonas Wäfler and Poul E. Heegaard

Norwegian University of Science and Technology  
N-7491 Trondheim, Norway  
{Jonas.Waefler, Poul.Heegaard}@item.ntnu.no

**Abstract.** The smart grid is a complex system consisting of interdependent power grid and information and communication (ICT) components. Complex systems have different properties than simple networks and give rise to new risks and failure types. In this paper, we study the dependencies in smart grid and the influence ICT may have on the dependability. We start with giving a categorization of the smart grid components and define state machines for these categories and for smart grid services. Then we investigate their interactions and interdependencies from a dependability perspective. Further, we investigate the positive and negative effects ICT can have on the dependability of the system. Finally, we introduce a meta-model which incorporates the information about the states of the components and services to create a state estimator for the smart grid considering ICT and power components.

## 1 Introduction

The reliability analysis of power grids has traditionally not included the state of supporting information and communication technology (ICT) infrastructure [1–3]. However, in the last ten years several authors pointed out the need of studying the power grid as complex network by including the cyber or ICT part in the analysis [1, 4, 5]. This complex network is called *cyber-physical* system or more general *system of systems*.

Theoretical results indicate the importance of analyzing the power grid (PG) and its supporting ICT together in one common model as a *system of systems*. It has been shown for interdependent random graphs that *system of systems* have different properties than simple systems [6]. Additionally, with an increasing number of interconnections and therefore a higher interdependency between the systems the vulnerability to random failures increases also [7].

A classification of particular types of failures which are caused by the interdependency of systems is put forward by [8]. Failures are classified as *cascading*, *escalating* and *common cause* failures depending on the interaction of the systems. Studies of major power grid incidents show that these interdependency effects between the PG and the ICT already exist in the current power grid [6, 9, 10]. A chain of cascading failures, i.e. failures in one system that trigger failures in another system, was a major reason for the large blackout in Italy in



2003 [6]. And an escalating failure, i.e. independent failures in the systems that amplify each other, was an important reason why the blackout in the US in 2003 could become so large [9]. Another analysis of the disturbances in the US power grid from 1979 to 1995 found that "*problems in real-time monitoring and operating control system, communication system, and delayed restoration contribute to a very high percentage of large failures*" [10]. The smart grid will rely even stronger on ICT than the legacy power grid, therefore, it can be expected that these effects will become even stronger.

The smart grid has the potential to increase the reliability of the power supply with new services like self-healing and demand response, which may reduce downtime and increase dependability [11]. However, misbehaving ICT and interdependency effects between ICT and PG have to be analyzed carefully and included into the dependability analysis, otherwise the results may be inaccurate and could lead to false conclusions about the system.

An interdependency model for the electricity and information infrastructure was presented in [12]. Using four to five different states for both infrastructures the model accommodates the three new failure types of *system of systems* as described in [8]. The model contains interesting features like passive and active latent errors; however, it is very high-level and the repair is not covered in details. Both power grid and ICT components are repaired in one step at the same time.

In 2009 an interdependency model for the power grid was put forward to illustrate the effect ICT can have on the reliability of the whole power grid [1]. In this model, both ICT and PG have a binary state variable and can either be in a normal or abnormal state leading to a four state model. The model is very conceptual and concentrates mostly on the transitions. Because of the high abstraction level most details are hidden within the states.

A more detailed approach is taken by [13] by introducing a three-level assessment hierarchical architecture consisting of a device, network and service level. Each level has its own properties and is modeled individually.

In this paper, we start bottom-up with the components constituting the smart grid and give a categorization based on their use of ICT. We then give state machines for the components and services and explain their interactions from a dependability perspective. Further, we discuss the positive and negative effects ICT can have on the dependability of the system. Finally, we introduce a meta-model which incorporates the information about the states of the components and services to create a state estimator for the smart grid considering ICT and power components.

## 2 Components and Services in the Smart Grid

The power grid consists of the power infrastructure on the one hand and of intelligent devices and a communication infrastructure to control and monitor it on the other hand. We categorize all components of the power grid into five categories as shown in Fig. 1. Category A contains power components with no communication means and no software like power lines and mechanical power

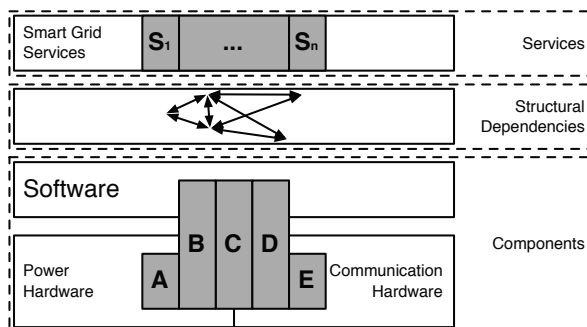


Fig. 1: Services and components of smart grids.

devices. Category B contains power components that are configurable but run autonomous and have no communication means like certain distributed energy resources. Category C contains software controlled power components with communication means like intelligent electronic devices used for monitoring and controlling the power grid. Category D contains software controlled communication components like routers. Category E contains communication components with no software like communication cables. It is important to note that some devices can be in several categories like a power cable which is also used as carrier of a PLC (power line communication) signal. Such structural dependencies can be the cause for common cause failures.

Devices in the categories B, C and D are in the following called intelligent devices. Components in A and E are called hardware (HW) components. Power HW components like power lines and transformers build the physical connections in the power grid between production sites and loads. The intelligent devices and the communication HW components are needed to operate the whole grid.

Smart grid services run on top of these components and they need a certain subset of components and other smart grid services to work. This partial dependency is called in the following *structural dependency*. The services are used to operate the power grid and include power delivery, monitoring, control, protection and more advanced services like demand response.

The biggest change in the transition from the legacy power grid to the smart grid will lie in the increase of software capabilities of B and C components and the quantitative increase of C components. In other words, the components become more intelligent and there will be more intelligent electronic devices to increase the system awareness and control, especially in the distribution grid. The latter will also lead to an increase of D and E devices in the smart grid. Additionally, the transition to the smart grid will change the power grid services. On the one hand, they are extensions to existing services like an increased monitoring and controlling in the distribution grid. On the other hand, they introduce new functionalities like smart metering or demand response.

## 2.1 State Machines for Components and Services

In the following we present state machines for components and services. The states are on a high level and different failure modes are not differentiated. For a quantitative analysis separate states for the considered failure modes have to be created and transition rates or probabilities assigned to the transitions.

Hardware components are modeled with two states as seen in Fig. 2. They can either be in a working state *ok* or a failed state *F*. Repair can happen after the monitoring system detected a failure or it can happen before when the failure is only temporary and disappears on its own.

Intelligent devices on the other hand, have a more complex failure behavior. First, we differentiate between *errors* and *failures*, as described in [14]. A fault can trigger an error in a device but only when the provided service is incorrect it becomes a failure. Differentiating errors and failures allows for example to model intermittent failures. While the failure disappears for some time, the responsible error does not. Second, a failure may be either passive ( $F_p$ ) or active ( $F_a$ ), depending on their behavior. We use the following definition similar to [12]:

**passive failure:** The device works incorrectly in a passive way, i.e. it does not respond when needed (e.g. not sending monitoring data, not responding to a control signal, not triggering a breaker when needed).

**active failure:** The device works incorrectly in an active way, i.e. it functions but not as intended (e.g. sending wrong monitoring data, executing the wrong control command, triggering self-healing when not necessary).

The corresponding errors are accordingly termed *passive errors* ( $E_p$ ) and *active errors* ( $E_a$ ). A device may also directly change its state from *ok* to  $F_p$  for example if parts of the hardware fail.

The devices are controlled by highly capable software which may cause harm to the system if working incorrectly. Due to the potential complexity of designing, configuring and updating such devices, faults are likely and errors may reside undiscovered in a device for a long time. Faults can be unintentional like design and configuration faults but also intentional like viruses/worms, intrusions and sabotage. Design, configuration or maintenance errors like software bugs, erroneous configuration/reconfiguration or the distribution of a faulty software update will affect potentially many devices at the same time. Failures may propagate on their own like in the case of a virus or a worm. The degree of the spreading depends on the detection and repair time.

The state of smart grid services may depend on the working and operational state of certain components, their structural dependencies, other services and on the input or the situation the system is in. The working states of a component are the states described above, the operational states are states in normal operation which can have an influence on a service. For example an open breaker which was opened by an undetected failure in an IED may cause the disconnection of parts of the grid and a state change for a service. The reason for the state change is the operational state of the breaker and only indirectly a failure. A service is said to be in the failed state *F* if the service produces incorrect output.

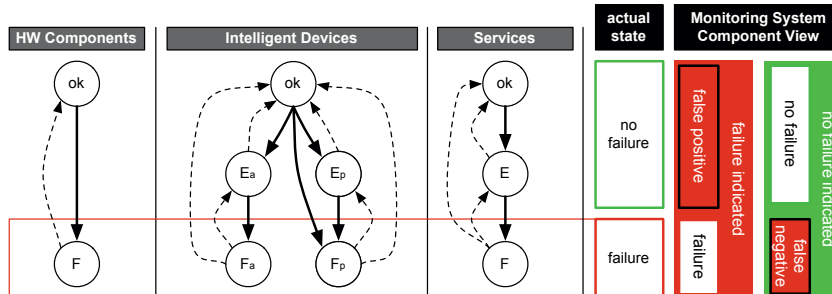


Fig. 2: State machines for components and services and the perception of their state in the monitoring system.

If components fail which are necessary to create correct output but the output itself is not yet incorrect, then the service is in the error state  $E$ . For example, consider a protection service which is responsible for opening breakers in a high overload situation. This service relies on protection devices installed throughout the power grid. The failure of one of these devices is already critical if there are no redundant devices. However, as long as there is no overload in which this specific device is needed to operate the service does not produce wrong output, hence the service is in the error state  $E$  while the device itself is in a failed state. In the error state the failure probability is much higher than in the working state. It is not the same as a failed state because for dependability analysis this state is considered as *not failed*. The monitoring system may detect the device failure and initiate the repair before the service fails.

## 2.2 Interactions

The components and services are highly depending on each other. The transitions between the states depend theoretically on the state of all the other components and services at a given time. For practical analysis of large systems the states may be modeled as depending only on the state of a subset of all components and services which are either geographically or logically close. In the following, we discuss the influence components can have on other components or services depending on their states.

### Influence of HW Components

**F** A failure may increase the load on other HW components and the probability for them to fail. This is especially the case for power HW components. Intelligent components may fail if a power HW component fails and there is no other power source (transition into  $F_p$ ).

### Influence of Intelligent Devices

**E<sub>a</sub> and E<sub>p</sub>** Errors have by definition no effect on other components.

**F<sub>a</sub>** An active failure may cause a change in the operational status in another component, e.g. opening a breaker, increasing power production instead of decreasing. This may lead to a critical situation and eventually even to a hardware failure or a service failure. An active failure may also cause errors and failures in other ICT components, e.g. by spreading harmful configuration or virus. It can also cause a smart grid service to not function properly.

**F<sub>p</sub>** A passive failure may cause a smart grid service to not function properly because for example necessary information is not delivered or information is not received and processed by the component. A passive failure may also lead to a failure in a power grid HW component, e.g. by not alarming the control center about a critical situation which could lead to an overload failure.

### Influence of Services

**E** An error has by definition no effect on other components or services.

**F** A failure can cause problems for the components or services relying on the output of this service. It may provoke a critical situation and eventually even to a failure in a component. For example, if the service *demand response* is increasing the loads instead of decreasing. If this happens in a distribution grid with a high number of charging electrical vehicles it could lead to an overload in that particular area and eventually even to a blackout, i.e. a failure of the power delivery service.

## 2.3 Perception of Components and Services

The monitoring system has its own perception of the system which is not the same as the actual state of the system. This is because the monitoring system is also just a service which can fail. The monitoring system can either indicate *failure* or *no failure*. The error states are considered as *no failure* as the delivered service is per definition still correct. As shown in Fig. 2 the indication can be wrong, i.e. be a *false positive* if a failure is indicated when there is none or be a *false negative* if no failure is indicated when there is indeed one.

The deviation of the indication in the monitoring system from the actual state is critical. If false positives are frequent it may cause high costs for the clarification of the cause and eventually to a loss of trust. False negatives may prolong the time a component or service stays in the failed state which decreases the dependability of the system. The longer a component is in the failed state the longer the negative interactions described above take place and more state changes in other components may happen.

## 2.4 Techniques for Quantitative Analysis

A difficulty when modeling the smart grid for quantitative analysis is that it consists of dynamic parts, i.e. the components with their state machines, and

structural parts, i.e. the structural dependencies between services and components. This becomes clearer when considering the smart grid services. The working and failed state of a given service may be described by a fault tree, where the events are failures of components or other services. This fault tree represents the structural dependency of the given service. The dynamic parts are the different failure modes leading to the events, i.e. failure of components or services.

A straight forward way of quantitatively analyzing a service is by creating markov models for each individual component and computing with them the dependability parameters needed for the fault tree. In this way, both availability and reliability of a service can be computed. However, this method assumes all events or state changes to be independent which is a very strong assumption and usually not true in real systems.

A way of including dependencies between components in an analytical model has been proposed in [15]. It starts with a reliability block diagram, i.e. a structural model which is equivalent to a fault tree and has the same independence assumption. The dependencies are then included by either isolating them or by using a combination of pivotal decomposition and markov chain. This method is most useful if the number of dependent components is small.

Another solution is to use a stochastic reward net (SRN) [16] which is an extension of a stochastic Petri net. The state machines from Fig. 2 can be used as a basis for the SRN in which the individual components and services are modeled as tokens. The transitions in SRN may be enabled by boolean functions on the markings of states and the transition rates may also depend on the marking of states. This allows to create a small model for a complex problem. However, this holds only if the components or services are treated as anonymous. If the identity of the different components and services become important, the model becomes more complex as well.

If the two mentioned methods are unpractical then a simulation may also be used for quantitative analysis.

### 3 Role of ICT in the Smart Grid

ICT components and services have a large potential for supporting the operation of a smart grid and increasing its dependability. The software part allows for smarter decision making processes and the communication allows for sharing information. Both are important for the most fundamental services: monitoring and controlling. An optimal monitoring system shows the actual state of the system with as little delay as possible and minimizes the discrepancy between perceived and real state. Precise data can help to operate the system in an optimal state and reduce errors and failures in the first place. For example, exact monitoring data in the distribution grid may optimize its use, maintenance and replacement, i.e. not wasting capacity or wearing the infrastructure unnecessarily out and preventively initiate repair or replacement before an incident happens. In case of a failure the monitoring service helps to detect and localize the failure. The reparation time may also be shortened by finding an optimal repair strat-

egy, by self-healing or by enabling the repair or mitigation by remote control, e.g. by isolating a line failure and possibly reconnect disconnected loads by an alternative route to reduce the impact of the failure.

By aggregating the data from the components new insights can be gained. For example, by finding patterns for failures which might improve error and failure prevention or failure detection. With a wide-area monitoring and control, enabled by communication, the optimal strategy for operation can be found for a certain area or the whole grid and not only for the local component. In case of an incident a coordinated protection or isolation scheme may prevent a propagation of the failure in the system.

While ICT can help to improve dependability, it can also have a negative effect. Passive failures in monitoring lead to a mismatch between perception and reality. A critical situation or failure may not be detected due to the missing data. In a controlling service a passive failure in a component leads to the disregard of the control signal. If no acknowledgment message is used this stays undetected and a mismatch between the assumed state of the component and the real state arises.

Passive failures reduce the potential improvement of ICT. The total failure of an ICT service nullifies its effect and intuitively one may conclude that additional ICT services will either improve the dependability of the whole system or at least keep the status quo. However, this is a dangerous conclusion because of two reasons. First, if services or controllers blindly rely on the service a passive failure may have a worse effect as not having the service at all. In the former case there is a strong assumption that the service works correct, in the latter case there is no correctness assumption and nobody is left with a false sense of security. Second, active failures may trigger new failures which would not exist without the specific service or ICT component.

Active failures in monitoring lead to a mismatch between perception and actual state and eventually even to undesired decisions and actions. For example, wrong information about the status of a breaker or the load of a line can trigger the isolation of a power grid part and lead to an unnecessary outage. Active failures in controlling lead also to a mismatch of perception and actual state but have in addition a direct effect on some components. Examples are protection devices initiating a protection process, breakers opening or closing, or the sending of wrong control signals. Frequent active failures of ICT components may negate the positive effect ICT can have and lead to an overall negative effect.

Last but not least, ICT plays a big enough role in the smart grid to qualify it as *system of systems*, which have particular interdependency effects and failure types, i.e. *Cascading Failure*, *Escalating Failure*, and *Common Cause Failure* [8].

## 4 Aggregated view for the Control Center

In the legacy power grid the control centers for the power grid and the communication system are usually separated. However, as new failure paths emerge in the smart grid which originate in or include ICT components, it becomes crucial

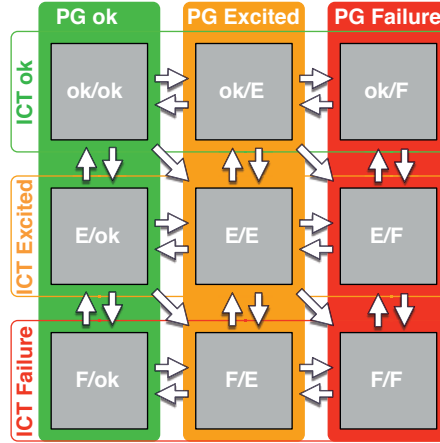


Fig. 3: Meta-model for smart grid.

to incorporate the information of both into the state estimation of the whole smart grid. This allows an early detection of possible failures coming from the ICT components.

In the following, we propose a meta-model to describe the state of the whole system for the control center. The meta-model is an aggregation and interpretation of the information from the monitoring system to determine the criticality level of the system. It has two axis using the states of the power grid (PG) and the ICT, see Fig. 3. The most important service in the power grid is the power delivery to the customers. The state of this service plus the state of supporting components are used to determine the power grid (PG) state. On the other hand, the states of ICT components and services are used together with a logic which indicates which services are critical to determine the state of the ICT system.

The model follows a service-centric approach. *Failure* means a service is not delivered correctly and action has to be taken immediately. *Excited* means that the service may run soon into a critical situation. More detailed, the states of the two axis are defined as:

**PG ok:** The system operates normally.

**PG Excited:** All customers are powered but the system is excited (N-1 redundancy is harmed, the load is critical, etc.)

**PG Failure:** At least one customer is disconnected from the power supply.



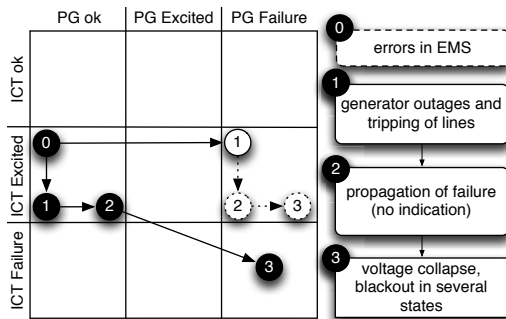


Fig. 4: Events in ICT and PG during an escalating failure in the US in 2003 as seen by the control center. The black disks indicate the information about the events as it happened. The white disks show how it could have been with a working detection mechanism, may be stopping the chain after event 1 or 2.

**ICT ok:** The ICT system operates normally.

**ICT Excited:** All critical ICT services are delivered correctly but the system is excited (non-critical components failed, congestion in the system)

**ICT Failure:** Some critical ICT services are incorrectly delivered.

The nine states are then created by the intersections of this two axis. Both excited states denote states of the system where the corresponding system is still working correctly but the stability and robustness is decreased. They are a key factor in the meta-model because the system may be much weaker than in the failure-free state and failures may propagate.

The states are as perceived by the control center and can be wrong as discussed above. These monitored states should be as close to the real states as possible. The fast detection of failures reduces the risk that the failure can propagate or cascade to other components. Monitoring should also be reliable to reduce the risk of having false positives and false negatives.

The meta-model is a highly condensed view of the whole grid to create a clear and easy understandable warning system. Due to the aggregation it is highly scalable. In large systems or in presence of autonomous structures like micro grids it may be useful to use several meta-models.

#### 4.1 Applications

The primary application for the proposed meta-model is the state indication of the smart grid for the control center as explained above. However, there are additional applications.

In ex post incident analysis the meta-model can be used to show the basic cause and effect chains in a clear way and study alternative scenarios. In Fig. 4 we give an example of such an analysis by showing the events of an escalating failure in the US in 2003 [9]. In short, several generators had an outage, which

led to a tripping of several lines. When that happened, the energy management systems (EMS) of the two responsible network operators were not fully functional and the failure could propagate in the PG and ended in a voltage collapse and a blackout spanning several federal states. In the figure, the black disks indicate the information the control center had during the events. The control center knew about the reduced functionality of the EMS but did not learn about the outage in the power grid until it was too late. The white disks indicate the information the control center would have had if the monitoring system had worked. The first outage could have been detected and the failure perhaps isolated which could have stopped the chain of events.

As an extension of the ex post incident analysis the meta-model can also serve as a tool to visualize and illustrate interdependencies in two systems. The new failure types propagation, escalation and common cause failures can be explained in an intuitive way and new failure paths are revealed.

## 5 Conclusion

The wide introduction of ICT changes the way the smart grid may fail. It is necessary to consider the states of both the ICT and the PG in the dependability analysis due to the following reasons:

- Dependability analysis for smart grid services yield inaccurate results if the possible non-functioning or malfunctioning of ICT is not included. ICT can have special dynamics like failure propagation within the system and active latent errors, which can have a strong effect on the smart grid.
- ICT plays a big enough role in the smart grid to qualify it as *system of systems*, which introduces particular interdependency effects and failure types. In individual models it is difficult to include those.

In this paper we categorized the smart grid components and services and showed the interactions between them. We motivated that their state and especially the state of the ICT components and services will play an important role in the dependability analysis of smart grids. We proposed a meta-model which takes this into account and combines the states of ICT and power grid components and services. It can be used as a tool for the control center to estimate the state of the smart grid. The proposed meta-model facilitates the understanding of the mechanisms of previous incidents by tracing their trajectories in the model. The simple structure creates an intuitive model that allows explaining the interdependencies and new failure types that are created by connecting systems. Understanding the risks is the first step to make a system more dependable and secure.

This work is meant to generally describe dependencies in the smart grid and to create a basis for future work. Future work will focus on specific interactions and interdependencies of components and services. We are especially interested in studying the new failure modes and evaluating and quantifying the dependability effects of new smart grid services.

## References

1. D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power and Energy Magazine*, vol. 7, no. 1, pp. 50–60, Jan. 2009.
2. A. Bose, "Models and techniques for the reliability analysis of the smart grid," in *Proc. IEEE PES General Meeting, Minneapolis, USA*, Jul. 2010, pp. 1–5.
3. C. Singh and A. Sprintson, "Reliability assurance of cyber-physical power systems," in *2010 IEEE PES General Meeting, Minneapolis, USA*, Jul. 2010, pp. 1–6.
4. M. Amin, "National infrastructure as complex interactive networks," in *Automation, control and complexity*, T. Samad and J. Weyrauch, Eds. New York, USA: Wiley, 2000, pp. 263–286.
5. R. G. Little, "Toward more robust infrastructure: Observations on improving the resilience and reliability of critical systems," in *Proc. of 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 2 - Volume 2*, 2003, pp. 58–66.
6. S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.
7. R. Parshani, S. V. Buldyrev, and S. Havlin, "Critical effect of dependency groups on the function of networks," *Proc. National Academy of Sciences of the United States of America*, vol. 108, no. 3, pp. 1007–1010, Jan. 2011.
8. S. Rinaldi, J. Peerenboom, and T. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, Dec. 2001.
9. G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.
10. Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.
11. V. V. Vadlamudi, R. Karki, G. H. Kjølle, and K. Sand, "Challenges in smart grid reliability studies," in *Proc. 12th Int. Conf. on Probabilistic Methods Applied to Power Systems (PMAPS), Istanbul, Turkey*, June 2012.
12. J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. SAFECOMP, Nuremberg, Germany*, 2007, pp. 54–67.
13. R. Zhang, Z. Zhao, and X. Chen, "An overall reliability and security assessment architecture for electric power communication network in smart grid," in *Power System Technology (POWERCON), 2010 International Conference on*, Oct. 2010, pp. 1–6.
14. A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Mar. 2004.
15. J. Wäfler and P. E. Heegaard, "A combined structural and dynamic modelling approach for dependability analysis in smart grid," in *Proceedings 28th ACM Symposium on Applied Computing (SAC), Coimbra, Portugal*, March 2013, pp. 660–665.
16. J. K. Muppala, G. Ciardo, and K. S. Trivedi, "Stochastic reward nets for reliability prediction," in *Communications in Reliability, Maintainability and Serviceability*, 1994, pp. 9–20.

---

# **A Combined Structural and Dynamic Modelling Approach for Dependability Analysis in Smart Grid**

Jonas Wäfler and Poul E. Heegaard

*Proc. 28th ACM Symposium on Applied Computing (SAC)*, Coimbra, Portugal,  
March 2013

© 2013, Association for Computing Machinery, Inc. Reprinted with permission.

Is not included due to copyright



---

# **Structural Dependability Analysis in Smart Grid under Simultaneous Failures**

Jonas Wäfler and Poul E. Heegaard

*Proc. IEEE Smart Grid Communications (SmartGridComm)*, Vancouver, Canada,  
October 2013

© 2013 IEEE. Reprinted with permission.





# Structural Dependability Analysis in Smart Grid under Simultaneous Failures

Jonas Wäfler and Poul E. Heegaard  
Department of Telematics  
Norwegian University of Science and Technology  
N-7491 Trondheim, Norway  
{jonas.waefler, poul.heegaard}@item.ntnu.no

**Abstract**—The pervasive use of information and communication technology (ICT) in the future power grid introduces new dependencies and new failure patterns. The simultaneous failure of several nodes may become more likely as devices get more complex and increasingly interconnected. Several studies investigated the behavior of power grids under simultaneous failures. However, the commonly used measure to quantify the outcome is agnostic to important characteristics of the power grid and its interpretation for dependability analysis remains unclear. We introduce two new measures which take the most fundamental characteristics of the power grid into account: the connectivity to power sources and the balancing of load and production. We analyze the two measures in scenarios with random and intentional node failures and conclude, that they are suitable for structural dependability and survivability analysis of power grids. Further, we use the new measures to quantify the potential dependability increase when using the smart grid services *Demand Response (DR)* and *Distributed Energy Resources* for failure mitigation. We find that a load reduction with DR by 20% may already achieve a large part of the possible dependability increase with *Demand Response*.

## I. INTRODUCTION

The future power grid will rely strongly on information and communication technology (ICT). Most proposed smart grid services build on a high density of intelligent electronic devices (IED) throughout the power grid and on a flexible communication platform [1]. This increasingly pervasive use of ICT enables new services and may increase the dependability of the future power grid [2], but it also increases the dependency on ICT and changes the way how dependability of power grids has to be assessed [3]. Failures in the future power grid may have their origin in failed ICT services. This chain of cause and effect is not new [4], [5] but it will have an even stronger impact in the future power grid.

IEDs contain embedded systems which may be highly configurable and together with the communication infrastructure it builds a system not unlike already deployed ICT systems. Highly configurable ICT systems are prone to human failures as indicated in the study of the US public switched telephone network where more than 50% of the failures were caused by humans by wrong maintenance, configuration or accidents [6]. Human made failures may be caused among others by the complexity of large networks with its various technical concepts, historically grown solutions, and its continuous renewal of technology [7]. Another study of critical infrastructures

in the US comes to the conclusion that more than 65% of all reported failures were software related, including software design, implementation, configuration, malicious logic fault inserted by an attacker, and authorization violation based on a faulty access control [8]. If these failures happen in IEDs it may lead to a failure in the power grid. Moreover, it is likely that several elements in the power grid are affected as they may have the same configuration or software implementation.

Studies on ICT networks indicate indeed that failures are not independent but rather correlated [9]–[11]. The reason may be:

- structural: subsystems share a common service or infrastructure (e.g. same configuration, sharing software update mechanism or using identical hardware)
- dynamic: a failure of one subsystem increases the stress on other subsystems
- epistemic: failures remain unobserved until a certain threshold is reached.

Correlated or simultaneous failures have been studied in various networks including the internet [12], [13] and power grids [14]–[17]. These studies model the simultaneous failure based on percolation theory which describes the behavior of the size of the largest connected network component after the removal of a fraction of  $1 - p$  of the  $n$  nodes of a network. A network component is a part of the whole network in which any two nodes are connected with a path and which is not connected to other nodes from the network. If a critical fraction of nodes  $1 - p_c$  is removed, the largest component collapses for a high number of nodes. The percolation point  $p_c$  and the size of the largest component after a failure of a fraction of  $1 - p$  nodes are used as indicators for the structural vulnerability or robustness. The latter is called in the following *Largest Component* measure and  $p$  goes usually from 0 to 1.

In [16] the relation of the percolation point  $p_c$  of 19 european transmission grids is investigated to non-topological reliability measures like average interruption time, power loss and energy not delivered. Dividing the grids into two groups based on the node degree distribution, they find a correlation between this grouping and the empirical reliability indices. However, it is not clear yet how to use this results for a classic dependability analysis as this *Largest Component* measure and its percolation point is agnostic to characteristics of the underlying network.

In [14] an additional measure is defined which takes connections between consumers and power sources into account. The number of power sources reachable from each node is counted before and after the incident and the averaged difference is then called *connectivity loss*. This measure yields less theoretic results as the *Largest Component* measure, however, it measures only the change and gives no indication about the number of disconnected nodes after the incident.

Several previous studies stressed the importance of adapting purely topological measures to the specifics of power grids and extended centrality measures with electrical parameters like impedance [18], impedance and power flow [19], electrical distance, power transfer distribution and line flow limits [20]. They have in common that they analyze the relative importance of nodes and lines with the aim to find vulnerable parts of the system.

In this work, we explore how network percolation can be used for structural dependability analysis of the future power grid. We introduce new measures taking fundamental properties of the power grid into account, i.e. the connectivity between consuming nodes and power sources on the one hand and balancing the consumption and production in connected network components on the other. The measures are used in scenarios with random failures and intentional failures. The results are compared with the *Largest Component* measure and analyzed for their suitability for dependability and survivability analysis. Further, we show how these new measures can be used to quantify the potential increase in dependability by using *Demand Response* and *Distributed Energy Resources* for the mitigation of the studied simultaneous failures.

## II. MEASURES

The quantification of the outcome of a failure in  $f$  of the  $n$  nodes can be done in different ways. The mentioned *Largest Component* measure is used widely. However, it relies entirely on the abstract indicator *largest component* and it is not immediately clear how to relate this to realistic dependability analysis. One may argue, that a power grid operator will not worry about the size of the largest component after an incident but rather about the number of customers experiencing a blackout.

We introduce two new measures which can be seen as an adaptation of network percolation to the needs of power grid dependability analysis. The main difference is, that all nodes of the network are considered, no matter how many components there are. All nodes are categorized as alive or not alive and the sum of all alive nodes gives then a dependability measure for the power grid. The definition of alive is done on power grid specific properties as explained in the next two subsections.

After an incident the network may be split into several network components. In the best case, all of the network components manage to pursue its operation independently in an island mode. In order to do that, several requirements have to be fulfilled. In the following we concentrate on the most fundamental ones: the structural requirements.

### A. Connectivity to power sources

The most fundamental requirement for a grid component to run as an island is, that it contains power sources, otherwise all its nodes experience a black-out. Using this key property of power grids a measure called *Connectivity* can be defined.

**Definition 1** (Connectivity). *Connectivity counts the number of alive nodes, i.e. nodes for which:*

- 1) *There is a path between the node and a power source.*

The measure indicates the number of nodes which could potentially be supplied with energy without repairing any parts of the network.

### B. Balancing production and load

The next requirement for a network component to survive as an island is, that the production capacity is high enough for the load of the connected nodes. It is assumed, that if the total load of a specific component is smaller than its maximal production capacity, the component may stabilize and continue operation as an island. If the load is higher than the maximal production capacity, it is assumed that breakers will open and disconnect loads until the total load of this network component is small enough.

In other words, the *Connectivity* measure is extended to consider also the production capacity of grid components.

**Definition 2** (Balancing). *Balancing counts the number of alive nodes, i.e. nodes for which:*

- 1) *There is a path between the node and a power source.*
- 2) *There is enough power production capacity for that specific node in the component. If the total production capacity of a component is too small for all the nodes, the number of alive nodes is continuously decreased by one until the load of the alive nodes is smaller or equal to the production capacity of the network component.*

The reduction of alive nodes can be done according to different strategies. We use a strategy that maximizes the number of supplied nodes. Other strategies could minimize the load not delivered or include priorities for critical customers like hospitals.

The measure indicates the number of nodes in the whole network which could be supplied with power in their respective component. The steps and the time used to increase the production to its potential and, if need be, to reduce the number of alive nodes, is outside of the scope of structural analysis.

## III. ANALYSIS AND DISCUSSION

### A. System Description and Modeling

The network used in this paper is based on a typical medium-sized regional grid from Norway with voltage levels 66 kV and 132 kV. It consists of transformer stations connecting to both the distribution grid and the transmission grid, power plants and interconnection points to other regional grids. We model it as a network with 104 nodes and 124 links, as depicted in Fig. 1. It is assumed that there exist

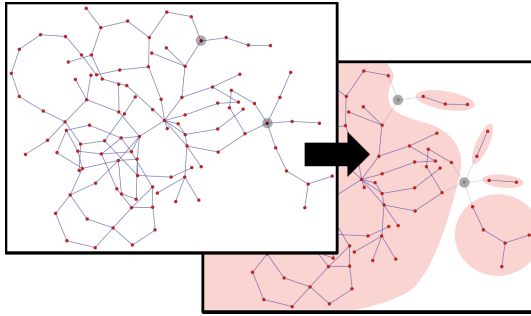


Fig. 1: Network based on typical medium-sized regional grid in Norway with an example simultaneous failure in 2 nodes (marked with grey disks). The resulting network is split into 5 network components after the failure (marked with red).

no other connections between the nodes than those depicted. Power sources are modeled by adding a production capacity to some nodes. For simplicity reasons, those nodes are in the following called power sources, even though several smaller power sources in the distribution grid could constitute the production capacity.

The modeled network has an average node degree of 2.38 which is higher than the node degrees of all 19 european transmission grids studied in [16]. The reason appears to be the higher node degrees of transformer stations in urban areas.

The considered incidents are simultaneous failures of  $f$  of the  $n$  nodes in the power grid. The nodes are modeled with a binary state, either the whole node is alive or it failed. Link failures are not included in our model because the main contributor for simultaneous failures is assumed to lie in the intelligent electronic devices (IED) in the nodes and not the links itself. Already today are failures in substations more frequent in the Norwegian power grid [21], however, the ratio *failures of links/failures in substation* varies strongly between different nations. It is important to note that the measures that will be discussed are agnostic to the failure cause. Test runs including link failures indicate similar results as for pure node failures.

The aim is to conduct a structural analysis of the power grid, i.e. an analysis of the structure ignoring power engineering challenges like stabilizing the frequency. Two different scenarios are considered. First, failure of  $f$  random nodes which models failures caused by unintentional faults like software faults, configuration faults or maintenance faults. Second, failure of  $f$  nodes chosen with a strategy to maximize the harm which models failures caused by intentional faults like a cyber attack. Repair is not considered in neither scenario.

### B. Simulation Setup

For this analysis, a snapshot of the system is considered in which the load is maximal and close to the maximal production of the power plants. All consuming nodes have the same power consumption and the consumption is assumed to be static.

All the producing nodes have the same production capacity. The total production capacity is 10% higher than the total load at this peak moment in the year. These assumptions are strong, but justifiable as the focus of this discussion lies on the measures. Moreover, this assumptions can easily be changed for a more realistic analysis of a given power grid.

Production capacity is assigned randomly to existing nodes in the network. The number of power sources in a power grid can vary widely depending on the topography but also strongly on the strategy of the utility and the government. To cover grids based on larger and smaller power plants, the simulation is run twice: for a power grid with 10 and for a power grid with 40 power sources.

A *Monte Carlo* simulation is used in which the number  $f$  of failed nodes goes from 1 to the total number of nodes in the network. The stochastic elements in the simulation are the location of power sources in the network and the location of failed nodes in the network.

### C. Random Faults

An incident is assumed that leads to the failure of  $f$  random nodes and their connected links in the network. The results in Fig. 2 shows the number of nodes which are considered alive according to the different measures.

The two newly introduced measures are closely related. The value for *Balancing* can never be higher than the value for *Connectivity* because the former is based on the latter and extends it by the requirement for enough capacity. The difference between the values depends on the ratio *total production/total consumption* which is set to 1.1 in this study. If this value increases, then the difference between the two curves will decrease and for very high values, which corresponds to almost no restriction from the production capacity, *Balancing* and *Connectivity* values will coincide.

The number of power sources in the system has a strong impact on the *Connectivity* and *Balancing* measures. If the number of power sources increases, the curve for the *Connectivity* measure tends to the diagonal, i.e. to a situation where the measure decreases linearly by the number of failed nodes. The *Balancing* curve will converge also to the diagonal if in addition the production capacity of the power source is at least as high as the consumption of the node it is attached to. The *Largest Component* measure does not consider this parameter.

For *Connectivity* and *Balancing* the 95% confidence interval shrinks when the number of power sources is increased. The difference between removing the most and least vulnerable nodes becomes less. This can also be seen in the next section when trying to remove the most vulnerable nodes first.

The measure *Largest Component* appears at first sight to be a conservative measure. However, this is not true because depending on the structure of the network the results can be higher than for the other two measures. For example, if there is only one power source in the network because in *Connectivity* and *Balancing* the power source may also be part of a minor network component. Another more realistic example is a grid which has all power sources clustered in a remote area and

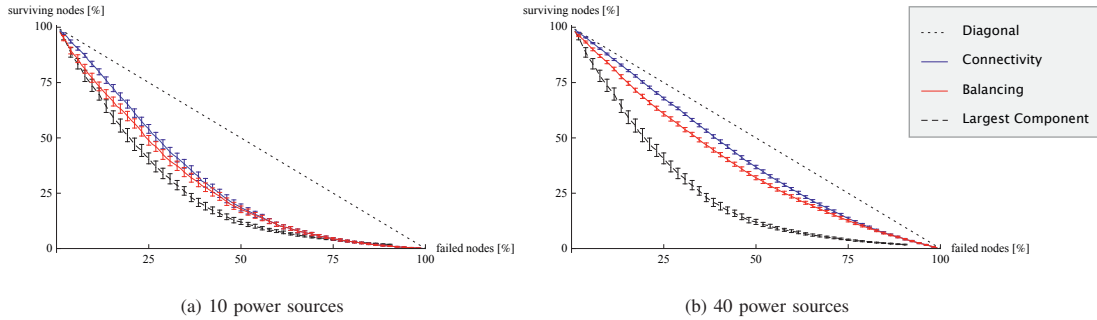


Fig. 2: Comparison of measures when performing random deletion of nodes. Results are mean values of 100 repetitions of a Monte Carlo simulation with randomly positioned power sources and random node failures. Whiskers indicate the 95% confidence interval for every second value. The dotted diagonal indicates the theoretic maximum for all measures.

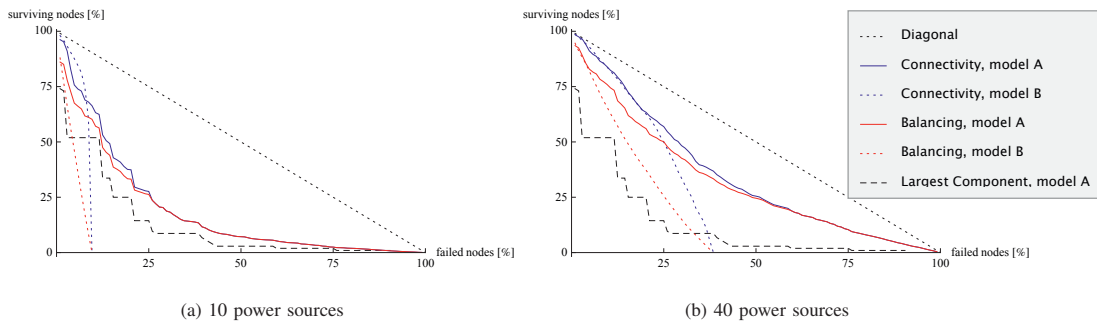


Fig. 3: Comparison of measures with intentional node failures. Results are mean values of 100 repetitions of a Monte Carlo simulation with randomly positioned power sources. The dotted diagonal indicates the theoretic maximum for all measures. The confidence interval is omitted to increase the readability.

they are connected only with few lines to the rest of the network with the consumers. If in addition the network part of the consumers is highly meshed then the results from the *Largest Component* measure will be higher than for the other two measures.

#### D. Intentional Faults

The previous experiment is repeated but now it is assumed that an attacker chooses which nodes should fail. Two different attacker models are used: In model A, the attacker chooses the  $f$  nodes with the highest node degrees in the network. In model B, the attacker chooses the  $f$  power producing nodes with the highest node degrees. Fig. 3 shows the results for the three discussed measures with the two attacker models. For the *Largest Component*, the data for model B is omitted because it is the same as for random faults, just stopping after  $x$  failures, where  $x$  is the number of power sources in the network. Using model A, there is no stochastic variance for the *Largest Component* because it is independent of power sources and the order for node failures is given by the strategy. The results will only change when the topology changes.

Considering only the *Connectivity* measure, the most harmful attacker model depends on the number of nodes which will

fail and on the number of power sources in the network. If both numbers are small then the attacker model A has a higher impact than attacker model B as can be seen from the results with 10 power sources. The consequences for the grid are higher when few nodes with a high node degrees are attacked than when the same number of nodes with power sources are attacked. In a highly connected network model B would yield a *Connectivity* result which decreases only by one until all power sources are deleted and the measure drops to 0.

For the *Balancing* measure it is slightly more complex because the ratio *total production/total consumption* has to be considered as well. As mentioned for the random failures, if this ratio grows, the results for *Balancing* tend to the results for *Connectivity* as the additional restriction from *Balancing* loses its importance for the result. For a larger number of failures model B is more harmful. If the number of power sources approaches the number of total nodes, as it is the case in a network with a high density of distributed energy resources, the results of the two strategies will converge. In general, the observation made for random failures are also valid here.

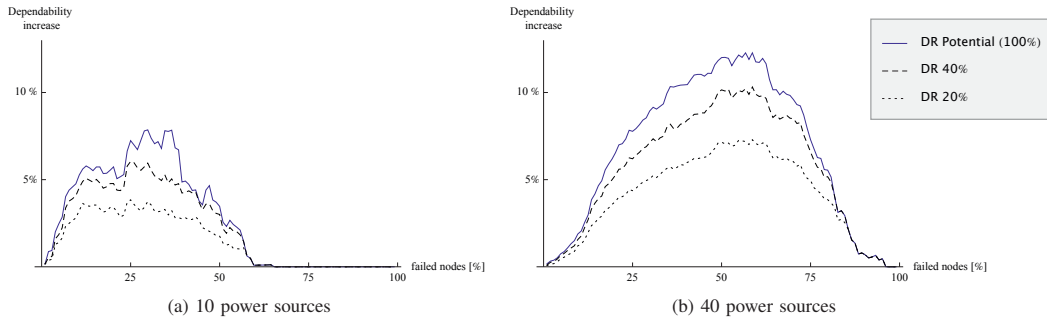


Fig. 4: Dependability increase by using different degrees of Demand Response (DR) to mitigate a simultaneous failure. Results are mean values of 100 repetitions of a Monte Carlo simulation with randomly positioned power sources and node failures

#### IV. SUITABILITY FOR DEPENDABILITY ANALYSIS

Dependability and Reliability terms are defined differently in power engineering and in ICT. Dependability in the ICT context is a general concept defined as “ability to avoid service failures that are more frequent and more severe than is acceptable” and it contains metrics like availability and reliability [22]. The former refers to the *readiness for correct service* and the latter to the *continuity of correct service*.

The *service* in a power grid is the power supply and *correct service* for a customer stands for no outage. Availability is then the probability that the customers experience no outage. In this context, the introduced *Connectivity* and *Balancing* measures quantify the instantaneous availability of the service after a simultaneous failure. If the failure and repair rates are known, then this can be used for the classic availability calculation for both dependability and security, dependent on the chosen failure model.

The measures can also be used for survivability analysis of a system. Survivability, closely related to dependability, is defined as the “system’s ability to continuously deliver services (...) in the presence of failures” [23]. The presented model corresponds to survivability without repair.

How to use the *Largest Component* measure for dependability analysis with the above definitions stays unclear because of the difficulty of defining *correct service* in a way that the results from this measure become meaningful. It is used as an indicator for topological robustness of a grid and even though [16] showed a correlation to statistical reliability measures it is easy to construct realistic scenarios where the results of *Largest Component* are misleading in the dependability analysis, as shown above.

In power engineering, reliability is defined as “degree to which the performance of the elements of that system results in power being delivered to consumers (...)”, this definition from NERC is also used by IEEE and CIGRE Working Groups [24]. If this *degree* of reliability is defined as *percentage of customers receiving correct service*, then this metric corresponds directly to the previous mentioned ICT availability.

#### V. ANALYSIS OF CONTRIBUTION OF SMART GRID SERVICES TO DEPENDABILITY

In the following, the measures are used to study the potential of two future smart grid services to mitigate the impact of the modeled simultaneous failure and increase thereby the dependability and survivability of the system.

##### A. Demand Response

Demand Response (DR) is a mechanism by which consumers change their consumption based on the price, the load or another signal [1]. In contrast to load shedding, an already existing method to reduce the load, DR reduces the loads without disconnecting customers. To study the potential of DR for failure mitigation it is important to consider the reason for a power loss in a node. According to the *Balancing* measure, a node can be non-functional because a) it was affected directly by the failure, b) it is part of a component without power source, or c) it is part of a component with too little power. The first two cases require repair. In the latter case, assuming a network-wide instantaneous and failure-free DR scheme, the load of the alive nodes can be reduced to supply non-functional nodes and turn them into alive nodes.

The two introduced measures may be considered as the two extreme cases of using DR, i.e. *Balancing* corresponds to *no DR* and *Connectivity* corresponds to 100% *DR* with no restriction on a minimal load per node. The difference between the measures is then the potential of DR. In Fig. 4 this potential is plotted together with the results when the load in each node is reduced by 20% and 40%. The y-axis shows the increase of the number of surviving nodes if DR is used. The results show that a DR scheme with 20% load reduction may achieve already around 50% of the total potential for DR under the taken assumptions. In countries with a high percentage of non-time critical loads like air conditioning or space and water heating, 20% or even 40% load reduction over a short period of time are realistic. The results depend on the ratio *total production/total consumption*. If this ratio is  $\approx 1$  or  $\leq 1$ , the potential for DR is large. If the ratio increases, the results of the two measures will get closer and the potential for DR will decrease.

### B. Distributed Energy Resources and Microgrids

Distributed energy resources (DER) are medium and small scale power sources located in any level of the power grid. The coordinated operation of DERs requires either a centrally located controller or a more local micro grid controller. The latter having the advantage of being able to run this part of the power grid in an island mode, speak as a decoupled micro grid [25], [26]. Micro grids are a mean to make parts of the grid independent from the functioning of the rest of the grid.

Assuming a high density of DER in the underlying distribution grid which are controlled by local micro grid controllers yields a scenario where the number of nodes with power sources is close to the number of total nodes. As seen in Fig. 2 and Fig. 3 increasing the number of power sources increases also the dependability of the network for both random and intentional node failures. The *Connectivity* measure approaches the diagonal because the probability that a network component ends up without a power source after the failure becomes smaller. The same holds to a lesser extent also for the *Balancing* measure. Assuming a failure-free operation of the micro grid controller, it can be concluded that DER and micro grids contribute to the mitigation of both random and intentional simultaneous failures.

### VI. CONCLUSION

Abstract measures from network science have been widely used for the analysis of power grids. They have the strong advantage of facilitating large scale studies and as they are agnostic to the underlying network they enable a comparison with other real-life or random networks. However, their meaning in the context of dependability and survivability analysis can be unclear and, therefore, have to be checked critically. In this paper, we introduced two measures based on fundamental properties of the power grid: connectivity to power sources and balancing of load and production. The analysis showed, that both new measures are well suited for a structural dependability and survivability analysis. In contrast to the widely used *Largest Component* measure which results can be misleading in this context.

Further, we showed how to use the measures to quantify the potential of *Demand Response* and *Distributed Energy Resources* to mitigate the consequences of simultaneous failures. Under the given assumptions, we found that a load reduction with DR by 20% can already achieve around half of the possible dependability increase with DR.

The structural analysis conducted in this study ignores dynamics in the system, however, the results give valuable information to power engineers about the upper limit of what can be achieved if all power engineering challenges are successfully met.

Future work will include the analysis of larger structures and possible failure mitigation strategies. Further, we will look into relaxing the assumptions to make the model more versatile.

### REFERENCES

- [1] International Energy Agency (IEA), "Technology roadmap: Smart grids," [www.iea.org/publications/freepublications/publication/smartgrids\\_roadmap.pdf](http://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf), 2011.
- [2] V. V. Vadlamudi *et al.*, "Challenges in smart grid reliability studies," in *Proc. 12th Int. Conf. on Probabilistic Methods Applied to Power Systems (PMAPS)*, Istanbul, Turkey, June 2012.
- [3] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power and Energy Magazine*, vol. 7, no. 1, pp. 50–60, Jan. 2009.
- [4] Z. Xie *et al.*, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.
- [5] G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.
- [6] D. Kuhn, "Sources of failure in the public switched telephone network," *Computer*, vol. 30, no. 4, pp. 31–36, Apr. 1997.
- [7] P. Cholda *et al.*, "Towards risk-aware communications networking," *Rel. Eng. & Sys. Safety*, vol. 109, pp. 160–174, January 2013.
- [8] H. A. Rahman *et al.*, "Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports," *Int. J. of Critical Infrastructures*, vol. 5, no. 3, Jan. 2009.
- [9] B.-Y. Choi *et al.*, "Outage analysis of a university campus network," in *Proc. 16th Int. Conf. on Computer Communications and Networks (ICCCN)*, Honolulu, Hawaii, 2007.
- [10] A. Gonzalez *et al.*, "Analysis of dependencies between failures in the UNINETT IP backbone network," in *Proc 16th IEEE Pacific Rim Int. Symp. on Dependable Computing (PRDC)*, Tokyo, Japan, Dec. 2010.
- [11] A. Markopoulou *et al.*, "Characterization of failures in an IP backbone," in *Proc. 23. IEEE INFOCOM, Hong Kong, China*, Mar. 2004.
- [12] R. Albert *et al.*, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000.
- [13] R. Cohen *et al.*, "Resilience of the internet to random breakdowns," *Physical Review Letters*, vol. 85, no. 21, pp. 4626–4628, Nov. 2000.
- [14] R. Albert *et al.*, "Structural vulnerability of the north american power grid," *Physical Review E*, vol. 69, no. 2, p. 025103, Feb. 2004.
- [15] M. Rosas-Casals *et al.*, "Topological Vulnerability of the European Power Grid under Errors and Attacks," *Int. J. of Bifurcation and Chaos*, vol. 17, no. 07, pp. 2465–2475, Jul. 2007.
- [16] R. V. Solé *et al.*, "Robustness of the european power grids under intentional attack," *Physical Review E*, vol. 77, no. 2, Feb. 2008.
- [17] Z. Wang *et al.*, "The node degree distribution in power grid and its topology robustness under random and selective node removals," in *Proc IEEE Int. Workshop on Smart Grid Communication (ICCS'10SGComm)*, Cape Town, South Africa, May 2010.
- [18] —, "Electrical centrality measures for electric power grid vulnerability analysis," in *Proc. 49th IEEE Conf. on Decision and Control (CDC)*, Atlanta, GA, 2010.
- [19] S. Arianos *et al.*, "Power grid vulnerability: A complex network approach," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 19, no. 1, pp. 013 119–013 119–6, Feb. 2009.
- [20] E. Bompard *et al.*, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, 2012.
- [21] European Network of Transmission System Operators for Electricity (ENTSO-E), "Nordic Grid Disturbance and Fault Statistics 2010," [https://www.entsoe.eu/fileadmin/user\\_upload/library/publications/entsoe/RG\\_SOC\\_Nordic/110831\\_NORDIC\\_GRID\\_DISTURBANCE\\_AND\\_FAULT\\_STATISTICS\\_2010.pdf](https://www.entsoe.eu/fileadmin/user_upload/library/publications/entsoe/RG_SOC_Nordic/110831_NORDIC_GRID_DISTURBANCE_AND_FAULT_STATISTICS_2010.pdf).
- [22] A. Avizienis *et al.*, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Mar. 2004.
- [23] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Computer Networks*, vol. 53, no. 8, pp. 1215–1234, 2009.
- [24] IEEE/CIGRE Joint Task Force on Stability Terms and Definitions, "Definition and classification of power system stability," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.
- [25] J. Driesen and F. Katiraei, "Design for distributed energy resources," *IEEE Power and Energy Magazine*, vol. 6, no. 3, pp. 30–40, 2008.
- [26] H. Jiayi *et al.*, "A review on distributed energy resources and Micro-Grid," *Renewable and Sustainable Energy Reviews*, vol. 12, no. 9, pp. 2472–2483, Dec. 2008.

PAPER **D**

---

# **Quantifying Influence of Strategies and Network Properties in Repairing Simultaneous Failures in Smart Grid**

Jonas Wäfler and Poul E. Heegaard

*Proc. Norsk Informatikkonferanse (NIK)*, Fredrikstad, Norway, Nov. 2014







# Quantifying Influence of Strategies and Network Properties in Repairing Simultaneous Failures in Smart Grid

Jonas Wäfler

Poul E. Heegaard

Norwegian University of Science and Technology

N-7491 Trondheim, Norway

{Jonas.Waefler, Poul.Heegaard}@item.ntnu.no

## Abstract

The behavior of networks under simultaneous failures has been subject to various studies in the field of network science. However, the measures used do usually not take into account the peculiarities of the studied network. In this paper, we introduce a new measure for power grids based on the balancing of power and on the accumulated cost of energy not supplied (CENS) during an outage. With the help of this measure we quantify the performance of seven repair strategies. We find that both the choice of the right strategy and the topology of the power grid has a major influence on the outage cost and the survivability of the power grid. Additionally, we appraise the potential of smart grid services and conclude that both distributed energy resources (DER) and demand response (DR) has a large potential to reduce the cost of an outage.

## 1 Introduction

Studies in information and communication technology (ICT) systems show the vulnerability of complex systems to human and software errors [1, 2] which may be caused, among others, by the complexity of large networks [3]. These errors affect potentially many devices as they run the same software, same configuration and are operated by the same humans. Studies indicate indeed that failures in ICT networks are not independent but rather correlated [4–6].

As the power grid relies more and more on the use of ICT [7], the dependency increases [8]. Failures in the power grid caused by failed ICT services are not new [9, 10] but they may become more frequent and exhibit a different pattern.

Correlated or simultaneous failures have been studied in various networks including power grids [11, 12]. These studies model the simultaneous failure based on percolation theory which describes the behavior of the network when removing

---

*This paper was presented at the NIK-2014 conference; see <http://www.nik.no/>.*

a fraction of  $1 - p$  nodes in a network. The most common measure to quantify the outcome of a simultaneous failure is to count the nodes in the largest connected component of the network, however, it is not clear how to use this results for a classic dependability analysis as this measure is agnostic to characteristics of the underlying network. Therefore, some measures were put forward considering connections between consumers and power sources [11, 13].

In this work, we analyze and compare several repair strategies to recover from simultaneous failures and quantify their performance during the repair time. In order to evaluate the different repair strategies we introduce a quantification method based on the accumulated cost of energy not delivered (CENS) during the repair. We consider the scenario in which the failure only affects the power grid and leaves the ICT system completely unaffected, i.e. the control center has the full information about the state of the whole network. We study how changes in the network, namely increasing the average node degree or increasing the number of power sources affect the repair costs. Further, we interpret our results in the advent of the smart grid services *Demand Response* and *Distributed Energy Resources*. And finally, we show how the results can be used for a survivability analysis.

Our analysis covers the repair of the physical structure of the power grid. We do not consider the restoration of the service, i.e. power delivery. The results give valuable information about the upper limit of what can be achieved if all power engineering challenges are successfully met.

## 2 Modeling

Our analysis takes place in regional grids with typical voltage levels of 66 kV and 132 kV. A regional grid consists of power plants, interconnection points to other regional grids, transformer stations connecting to both the distribution grid and the transmission grid, and lines and cables connecting all these entities. The network is modeled as an undirected graph in which all the mentioned entities are modeled as nodes and the lines and cables are modeled as links between the nodes. The lower voltage levels with the consumers are not included in the model. However, the nodes have a load and power production corresponding to the sum of all the loads or power production connected to them. All nodes have a load, some nodes have additionally an attached power production, these nodes are called power producing nodes or power sources. We do not differentiate whether the power production is the sum of several smaller power sources in the distribution grid or one large power plant. Neither differentiate we between power plants, connections to the transmission grid and interconnections to regional grid. Important is only the sum of the power production. It is assumed that there exist no other connections between the nodes than those in this voltage level, i.e. in the network.

### Cost of Energy Not Supplied (CENS)

In regulated networks, the regulator gives incentives for efficient and reliable operation of the grid. In the following we use the Norwegian regulation framework based on a yardstick regulation where the performance of a utility is measured in comparison with the others. Cost of Energy Not Supplied (CENS) is one parameter used for the efficiency and cost calculations for the revenue cap [14]. CENS is calculated by a function taking as input the *power not supplied* to a customer and the *time of the outage*. There exists a function for each customer group as listed

Table 1: Cost functions and groups used for the CENS calculation (Unit: Norwegian Krone /kW).

Customer group	original cost function depending on outage time $r$		average cost function used in sim.	share of customer
	$r \leq 4h$	$r > 4h$		
Agriculture	$10.6r + 4$		62.3	4%
Residential	$8.8r + 1$		49.4	75%
Industry	$55.6r + 17$	$18.4r + 166$	244.8	1%
Commercial	$97.5r + 20$	$33.1r + 280$	422.45	10%
Public	$14.6r + 1$	$4.1r + 44$	59.85	10%

in Table 1. In the simulation we do not consider outage times, therefore, we use a time independent cost function, which depends only on the *customer group* and on the *power not supplied*. The value used in our cost function is the expected value of the time-depending cost function under the assumption that the outage times are uniformly distributed and take integer values between 1 and 10 hours. More details about CENS can be found in [14].

The nodes in the network have no CENS values themselves because they are substations and not customers. However, the sum of the CENS values of all customers connected to a node is taken as the CENS value for that node. It is assumed that all nodes have the same load and each node has only customers of the same group attached. To calculate the cumulative CENS for a network node we can use its cumulative load and use the cost function with the CENS parameter for the corresponding group.

### Failure and Repair

The nodes are modeled with a binary state, either the whole node is alive or it has failed. Link failures are not included in our model. The ratio (*link failures*)/(*substation failures*) varies strongly between different nations [15].

The considered failure is a simultaneous failure of a fraction of  $f$  nodes. The set of failed nodes is denoted as  $V_{failed}$ . A failure can lead to a supply shortage or disconnection of additional nodes leaving the network with a total of  $s\%$  of nodes non-alive. The set of non-alive nodes is in the following denoted  $V_{non-alive}$ . The sets have the properties:  $|V_{failed}| = fn$ ,  $|V_{non-alive}| = sn$  and  $V_{failed} \subseteq V_{non-alive}$  where  $n$  is the total number of nodes in the network.

The considered repair mode is a one-by-one repair, i.e. only one failed node at a time can get repaired. In each repair step one node is chosen according to a strategy and repaired. It is assumed that the repair is successful and that no additional failures happen during the repair. All repair strategies start with  $|V_{non-alive}|$  non-alive nodes and end after  $|V_{failed}|$  repair steps because only the failed nodes need to be repaired. However, the order of repairing the nodes has an impact on how many nodes of the network are alive as repairing the right node may bring back the power supply to many other nodes as well.

## 3 Simulation Setup

The simulation covers only the repair process. A snapshot of the system is considered in which the load is maximal and close to the maximal production of the power

plants. All consuming nodes have the same power consumption and the consumption is assumed to be static. All the producing nodes have the same production capacity. The total production capacity is 10% higher than the total load at this peak moment in the year. These assumptions are strong, but justifiable as the focus of this discussion lies on the strategies. Moreover, these assumptions can easily be changed for a more realistic analysis of a given power grid.

This *Monte Carlo* simulation has as stochastic variables the location of power sources, the location of failed nodes and the assignment of CENS customer groups to the nodes. The first two use a uniform distribution, the last a distribution with the expected values from Table 1. All stochastic variables change in each repetition.

During the analysis two different networks are used. First, a network based on a typical medium-sized regional grid from Norway with voltage levels 66 kV and 132 kV. It consists of 104 nodes and 124 links. Second, a network randomly generated with a node degree distribution that follows an exponential distribution. It has been shown in a study that the European transmission networks possess this property [12].

To cover grids based on larger centralized and smaller decentralized power plants, the simulation is run for two parameters: for a power grid with 10 and for a power grid with 40 power sources.

The ICT network is completely independent from the power grid and it is assumed to work flawlessly also after the failure in the power grid happened. The control center has therefore a full and correct overview over the system and knows which nodes belong to the set of non-alive nodes  $V_{non-alive}$  and also which nodes belong to the set of nodes with a failure  $V_{failed}$ . The former gives information about the extent of the outage, the latter the valuable information about which nodes need to be repaired. As all the information is available only the order of repairing the nodes has to be determined by a chosen strategy. We consider the following strategies to choose the next node to repair:

1. *Baseline for comparison:*
  - (a) *Random Repair:* Choose a random node from  $V_{failed}$ .
2. *Strategies based on properties of single nodes:*
  - (a) *Highest Node Degree:* Choose the node with the highest node degree, i.e. the most links, in  $V_{failed}$ .
  - (b) *Highest CENS:* Choose the node with highest CENS value in  $V_{failed}$ .
3. *Strategies optimizing outcome of next step:*
  - (a) *Maximize Node Count:* Choose the node from  $V_{failed}$  which maximizes the number of alive nodes. The algorithm simulates all possibilities for the next step and takes the one giving the highest result.
  - (b) *Minimize CENS:* Choose the node from  $V_{failed}$  which minimizes the CENS costs for the next step. The algorithm simulates all possibilities for the next step and takes the one giving the lowest result.
4. *Strategies based on properties of connected component:*

- (a) *Biggest Failed Component*: Consider the graph formed by the nodes in  $V_{non-alive}$  and choose the biggest connected network component. Consider all nodes from that component which are in  $V_{failed}$  and take the one with the highest node degree.
- (b) *Failed Component with Highest CENS sum*: Consider the graph formed by the nodes in  $V_{non-alive}$  and choose the one with the highest sum of the CENS values of its nodes. Consider all nodes from that component which are in  $V_{failed}$  and take the one with the highest node degree.

The strategies are chosen in a way to study the influence of considering *single nodes* versus *connected components*, and *node or degree count* versus *CENS values*. After the random strategy, which is used for comparison, there are three pairs of strategies. The strategies from the first pair consider only properties of single nodes for their decision, the strategies from the second pair consider the outcome of all possible repair steps and take the optimal solution and the strategies of the last pair base their decision on connected components of nodes in  $V_{non-alive}$ , i.e. they consider also the non-alive nodes that have no failure. In each pair there is one strategy considering only topological aspects like node degree or node count and one strategy considering CENS.

## Measures

In the following, we use the two measures proposed in our previous work [13] to quantify  $V_{non-alive}$ : *Connectivity* counts the number of nodes still connected to any power source, *Balancing* requires in addition that the sum of loads in a surviving connected network component is at maximum equal to the sum of power production in that component. If the load is too high, loads are shut down.

When considering the financial impact of an outage for the responsible utility it becomes important *which* nodes are non-alive and not only *how many*. Therefore, we extend the measures to include the financial impact of the whole outage.

**Definition 1** (CENS outage cost). *The CENS outage cost is the sum of the CENS values of all the non-alive nodes, summed up over all repair steps. The non-alive nodes are determined with either the Connectivity or Balancing measure.*

## 4 Simulations and Results

### Performance of Strategies

We first investigate the performance of the previously introduced strategies. The simulation is run with the network based on the described Norwegian regional grid. The results of 100 simulation runs are given in the lower row of Fig. 1. The best performing strategy, i.e. the strategy that leads to the lowest *CENS outage costs* is the *Minimize CENS* strategy. This is not surprising, as it optimizes the outcome for the next step. The *Maximize Node Count* strategy performs reasonably well considering that it is agnostic of the CENS values of the nodes. Although, for a higher number of power sources (40) the difference becomes bigger. The other five strategies are more than 50% more expensive than the best one. For a low number of power sources the difference is even slightly higher.

The strategies *Highest Node Degree* and *Biggest Failed Component* consider only topological aspects. They both have a similar performance. Taking into

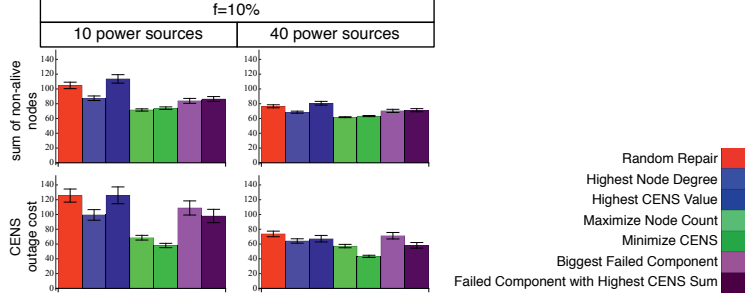


Figure 1: CENS outage costs in the regional grid model when 10% of the nodes fail. In the left column 10 nodes have attached power sources, in the right column 40 nodes have attached power sources. The upper row shows the sum of non-alive nodes over the whole repair process and the lower row shows the sum of CENS values of all non-alive nodes over the whole repair process (*CENS outage cost*) for the different strategies. The non-alive nodes are determined with the *Balancing* measure. The results are mean values of 100 repetitions of a Monte Carlo simulation with randomly positioned power sources and random failures. Whiskers indicate the standard error of mean.

account groups of nodes from  $V_{non-alive}$  like in *Biggest Failed Component* brings no advantage against considering only single nodes from  $V_{failed}$  like in *Highest Node Degree*, it yields even a slightly worse performance. The opposite is true for the two strategies considering only the CENS values. Here the strategy taking into account components of nodes from  $V_{non-alive}$ , i.e. trying to reconnect the component with the highest CENS sum (*Failed Component with Highest CENS Sum*) performs better than the strategy *Highest CENS Value* which considers only single nodes from  $V_{failed}$ .

### Comparing CENS outage cost with Node count

A simple measure to quantify a repair strategy could be to count the number of non-alive nodes per repair step and then sum it up. The proposed measure *CENS outage cost* takes the additional information about the CENS values into account, which is not directly topology related. Using this new measure we try to find a strategy that minimizes this *CENS outage cost*. It may seem wrong to use a financial parameter to measure the performance of repair strategies, but the CENS values can also be understood as a criticality indication of the nodes. In order to check the implications on the availability of the nodes, we run the same simulations with all strategies and measure it with the purely topological measure *sum of non-alive nodes* and also with the measure *CENS outage cost*. The results are presented in Fig. 1. The strategy *Maximize Node Count* optimizes the first measure, the strategy *Minimize CENS* optimizes the second measure. The results show, that those two strategies perform very similar when using the first, topological measure, i.e. optimizing for CENS values optimizes also the sum of non-alive nodes. However, this is not the case for the second measure. The difference between the two strategies becomes bigger with a higher number of power sources. The same is true for the two last strategies focusing on components on either the topological level or the CENS level. The statistical relevant differences are smaller here. Interestingly this is not true

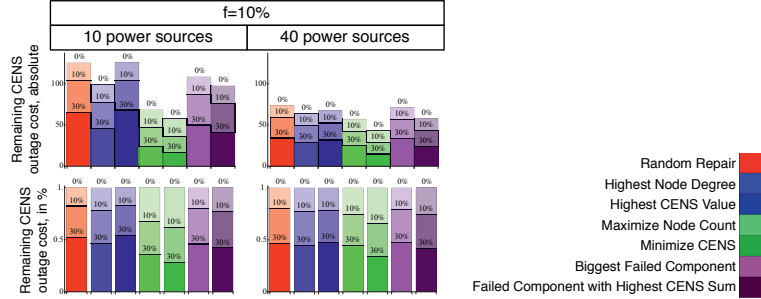


Figure 2: Remaining costs *before* repairing, after having repaired 10% of the failed nodes, after having repaired 30% of the failed nodes in the regional grid model. The upper row gives the absolute value for CENS, the lower row gives the remaining outage costs after in percentage of the total costs. The non-alive nodes are determined with the *Balancing* measure. The results are mean values of 100 repetitions of a Monte Carlo simulation with randomly positioned power sources and random failures.

for the first pair of strategies after the random strategy. Using the *Highest Node Degree* strategy is for both measures better than using the *Highest CENS Value*. The difference to the other two strategies using CENS is, that the two latter consider the CENS-sum of a group of nodes which includes also a topological aspect, therefore, they also perform well compared to their topological counterparts using the sum of non-alive nodes measure.

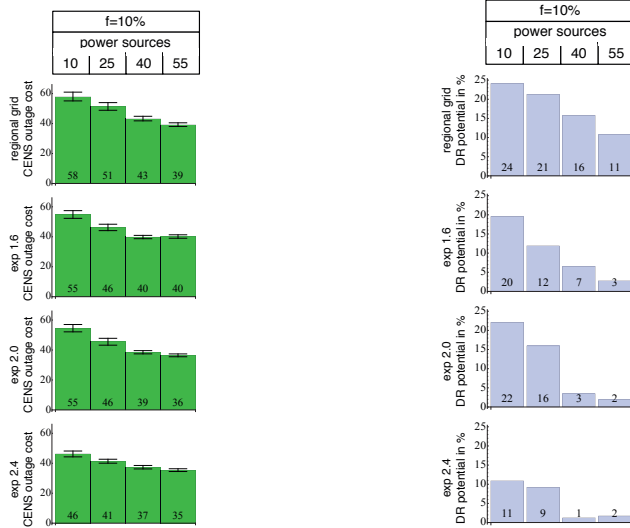
As conclusion we can state that using the best strategy *Minimize CENS* reduces the costs without increasing the number of non-alive nodes compared to the strategy *Maximize Node Count*. This can be done because optimizing for a minimal CENS implicitly also favors a small number of non-alive nodes. The utility can here reduce costs without sacrificing the availability of its nodes.

### Cost Development of Strategies

In our model the repair takes always the same amount of steps, each strategy needs to repair  $|V_{failed}|$  nodes. But depending on the strategy the degree to which the service is back will be different. In Fig. 2 we have plotted the remaining *CENS outage cost* after having repaired 0%, 10% and 30% of the failed nodes. The strategy with the lowest absolute *CENS outage cost* also has the property of reducing the cost faster. In the scenario with 10 power sources, the best strategy *Minimize CENS* reduces the *CENS outage cost* by 30% by repairing 10% of the failed nodes, i.e. by repairing one single node. After repairing 2 additional nodes (in total 30% of the nodes) only 1/3 of the total *CENS outage cost* remain. The results illustrate that repairing with the right strategy can reduce the costs drastically.

### Influence of Node Degree and Number of Power Sources

In the following we study the effect of increasing the number of power sources. As before the regional grid is used with randomly positioned power sources and a random node failure of 10% of the nodes. The number of power sources takes the values 10, 25, 40 and 55. Only the best strategy *Minimize CENS* is considered.



(a) *CENS outage cost* in the regional grid and in random networks whose node degrees follow an exponential distribution  $exp(\lambda)$  with  $\lambda \in \{1.6, 2.0, 2.4\}$ . The repair strategy *Minimize CENS* is used after 10% of the nodes failed. The non-alive nodes are determined with the *Balancing* measure. Whiskers indicate the standard error of mean.

(b) DR potential to reduce *CENS outage cost* in the regional grid and in random networks whose node degrees follow an exponential distribution  $exp(\lambda)$  with  $\lambda \in \{1.6, 2.0, 2.4\}$ . The repair strategy *Minimize CENS* is used after 10% of the nodes failed.

Figure 3: The results are mean values of 100 repetitions of a Monte Carlo simulation.

Additionally we use random networks whose node degrees follow an exponential distribution  $exp(\lambda)$  with  $\lambda \in \{1.6, 2.0, 2.4\}$ . The simulation results are shown in Fig. 3a. For all four networks the *CENS outage cost* goes down when the number of power sources increases. Increasing  $\lambda$ , which increases the average node degree, reduces the *CENS outage cost* as well. However, this effect is stronger for a small number of power sources in the network. If the number of power sources increases even more the difference disappears completely as can be seen when considering the case when all nodes have a power source. Then, the node degree of the nodes has no influence anymore as each node is self-contained.

Utilities have two ways of reducing *CENS outage cost*: First, by increasing the average node degree. Second, by increasing the number of power sources. The former is very expensive, usually not practical because of restrictions for building new links and as shown in the results less effective than the latter.

## 5 Discussion

The results show that choosing the right strategy can reduce the costs of an outage drastically. The best strategy is the one finding the optimal solution for the next



step, i.e. it simulates all possibilities for the next step and chooses the one with the best outcome. The computational complexity is higher than with the other strategies, but this is not an issue as the number of possibilities is only as large as the number of failed nodes. In our examples, the simulation runs could be executed very quickly, the simulation finished in a matter of milliseconds on a normal desktop computer and is several orders of magnitude smaller than the actual repair time. The network type, the average node degree and the number of power sources has an influence on the total *CENS outage cost*. Usually those parameters cannot be changed in a power grid. However, with the advent of smart grid with its new services two things may change:

1. The number of power sources may change drastically as small and distributed power sources (DER) are promoted.
2. A *Demand Response* (DR) scheme may reduce the load.

The results can be used to appraise the potential to reduce the cost of outages by using these two smart grid concepts.

### **Impact of Distributed Energy Resources on Outage Costs**

Distributed energy resources (DER) are medium and small scale power sources located in any level of the power grid. The coordinated operation of DERs requires either a centrally located controller or a more local micro grid controller. The latter having the advantage of being able to run this part of the power grid in an island mode, i.e. a decoupled micro grid [16, 17]. Micro grids are a mean to make parts of the grid independent from the functioning of the rest of the grid. Assuming a high density of DER in the underlying distribution grid which are controlled by local micro grid controllers yields a scenario where the number of nodes with power sources is high. As seen in Fig. 3a increasing the number of power sources reduces the *CENS outage cost*. We can, therefore, conclude that DER reduces the *CENS outage cost* and it can even be quantified by using the introduced measure.

### **Impact of Demand Response on Outage Costs**

Changing topological parameters or the number of power plants is in reality either unrealistic or connected with potentially high costs. Instead, the existing infrastructure may be used more efficiently; one solution is to use *Demand Response* (DR). DR is a mechanism by which consumers change their consumption based on the price, the load or another signal [7]. In contrast to load shedding, i.e. disconnecting loads to achieve the power balance, DR reduces the loads without disconnecting nodes. In a scenario with a high density of distributed power production and energy storage, DR may also control the distributed production or feeding of power from the storages to the grid. However, we do not consider the control of production by DR in this paper. A DR scheme has the advantage of using the existing infrastructure in a more efficient way by regulating the load. This is also linked with costs to install the DR infrastructure like devices and a communication platform. But as the new infrastructure is also used by other smart grid services like monitoring and controlling the costs can be split.

To study the potential of DR for reducing outage costs it is important to consider the reason for a power loss in a node. According to the *Balancing* measure, a node

can be non-functional because a) it was affected directly by the failure, b) it is part of a component without power source, or c) it is part of a component with too little power. The first two cases require repair. In the latter case, assuming a network-wide instantaneous and failure-free DR scheme, the load of the alive nodes can be reduced to supply non-functional nodes and turn them into alive nodes.

The measures *Balancing* and *Connectivity* may be considered as the two extreme cases of using DR, i.e. *Balancing* corresponds to *no DR* and *Connectivity* corresponds to 100% *DR* with no restriction on a minimal load per node. The difference between the measures is then the potential of DR. In Fig. 3b this potential is plotted, i.e. the reduction of *CENS outage cost* when the whole DR potential could be used compared to no DR.

The results show that the DR potential is highest for a low number of power sources in the network. Increasing the node degree leads to a decrease in DR potential as the probability that a network component is without a power source becomes smaller. In the extreme case of a complete graph the potential disappears completely as the nodes are not dependent on the load of other nodes anymore. The same holds for the case when the number of powered nodes goes to 100%.

The results depend on the ratio  $(total\ production\ capacity)/(total\ consumption)$ . If this ratio is close to 1 or even smaller than 1, the potential for DR is large. If the ratio increases, the results of the two measures will get closer and the potential for DR will decrease.

## Survivability Contribution of Strategies

Dependability is defined as “*ability to avoid service failures that are more frequent and more severe than is acceptable*” and it contains metrics like availability and reliability [18]. A related measure is *survivability* which is defined as “*system’s ability to continuously deliver services (...) in the presence of failures*” [19]. It can also be understood as how fast and to what degree the service is still delivered or restored after a failure. The CENS value has been introduced with the objective “*to achieve the most optimal level of continuity of supply for the society as a whole*” [14]. Therefore, it can be understood as a criticality indicator of the node. The *CENS outage cost* is then a measure for how well the continuity of supply has been provided during the repair, or in other words it measures the survivability. The lower the value, the higher its survivability. To get more details for the survivability analysis it is necessary to investigate the development of service restoration; a highly survivable system should restore the most critical parts first. These information can be found in Fig. 2, which shows the development of the *CENS outage cost* for the different strategies. The results can be directly applied to survivability analysis, i.e. using the right strategy increases the survivability drastically.

Assuming we include time as a factor, we can also state that it is most crucial to have short repair times for the first nodes. For the second half or even for the second 2/3 of nodes time is not so crucial anymore, as the most critical nodes are already repaired.

## 6 Conclusion

Simultaneous failures have been studied in various networks in the field of network science. These abstract results can be used for power grids, however, it is crucial to

tailor them to the specific peculiarities of the system. In this paper, we introduced a measure based on CENS values of power grid nodes and on the *Balancing* measure. The new measure allowed us to quantify and compare the performance of different repair strategies and networks. As CENS has a direct impact on the regulated tariffs of a utility it is an important parameter to consider in the event of an outage but especially also for determining the order of repairing the nodes. CENS was introduced specifically as a sort of criticality value for each node and to give incentives to prioritize certain customer groups.

The results show that using the strategy minimizing the CENS costs for the next step has various advantages. First, it performs comparably to the strategy *Maximize Node Count* when using the node count measure. Second, it reduces the *CENS outage cost* considerably compared to the CENS-agnostic strategies. Third, it improves the survivability by restoring critical nodes faster.

We could also show that increasing the average node degree of a network reduces the *CENS outage cost*. However, increasing the number of power sources leads to an even stronger improvement and reduces the difference between networks of different average node degrees. Thus, increasing the number of power sources is the less expensive way of reducing the *CENS outage cost*. In smart grid terminology this indicates that DER reduces the *CENS outage cost*. And finally, we showed that a DR scheme has the potential of reducing the *CENS outage cost* by up to 24%.

The structural analysis conducted in this study concentrates on the structure of the power grid and its repair. We do not consider the service, i.e. power delivery and, therefore, dynamics in the system are not included. The results give valuable information to power engineers about the upper limit of what can be achieved if all power engineering challenges are successfully met.

## References

- [1] D. Kuhn, "Sources of failure in the public switched telephone network," *Computer*, vol. 30, no. 4, pp. 31–36, Apr. 1997.
- [2] H. A. Rahman, K. Beznosov, and J. R. Marti, "Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports," *Int. J. of Critical Infrastructures*, vol. 5, no. 3, Jan. 2009.
- [3] P. Cholda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, and I. Norros, "Towards risk-aware communications networking," *Rel. Eng. & Sys. Safety*, vol. 109, pp. 160–174, January 2013.
- [4] B.-Y. Choi, S. Song, G. Koffler, and D. Medhi, "Outage analysis of a university campus network," in *Proc. 16th Int. Conf. on Computer Communications and Networks (ICCCN), Honolulu, Hawaii, 2007*.
- [5] A. Gonzalez, B. Helvik, J. Hellan, and P. Kuusela, "Analysis of dependencies between failures in the UNINETT IP backbone network," in *Proc 16th IEEE Pacific Rim Int. Symp. on Dependable Computing (PRDC), Tokyo, Japan, Dec. 2010*.
- [6] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot, "Characterization of failures in an IP backbone," in *Proc. 23. IEEE INFOCOM, Hong Kong, China, Mar. 2004*.


- [7] International Energy Agency (IEA), “Technology roadmap: Smart grids,” [www.iea.org/publications/freepublications/publication/smartgrids\\_roadmap.pdf](http://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf), 2011.
- [8] D. Kirschen and F. Bouffard, “Keeping the lights on and the information flowing,” *IEEE Power and Energy Magazine*, vol. 7, no. 1, pp. 50–60, Jan. 2009.
- [9] Z. Xie, G. Manimaran, V. Vittal, A. G. Phadke, and V. Centeno, “An information architecture for future power systems and its reliability analysis,” *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.
- [10] G. Andersson *et al.*, “Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance,” *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.
- [11] R. Albert, I. Albert, and G. L. Nakarado, “Structural vulnerability of the north american power grid,” *Physical Review E*, vol. 69, no. 2, p. 025103, Feb. 2004.
- [12] M. Rosas-Casals, S. Valverde, and R. V. Solé, “Topological Vulnerability of the European Power Grid under Errors and Attacks,” *Int. J. of Bifurcation and Chaos*, vol. 17, no. 07, pp. 2465–2475, Jul. 2007.
- [13] J. Wäfler and P. E. Heegaard, “Structural dependability analysis in smart grid under simultaneous failures,” in *Proc. IEEE Smart Grid Communications (SmartGridComm)*, Vancouver, Canada, October 2013.
- [14] G. Kjølle, K. Samdal, and K. Brekke, “Incorporating short interruptions and time dependency of interruption costs in continuity of supply regulation,” in *CIREC, Prague, Czech Republic*, 2009, pp. 1–4.
- [15] European Network of Transmission System Operators for Electricity (ENTSO-E), “Nordic Grid Disturbance and Fault Statistics 2010,” [https://www.entsoe.eu/fileadmin/user\\_upload/\\_library/publications/entsoe/RG\\_SOC\\_Nordic/110831\\_NORDIC\\_GRID\\_DISTURBANCE\\_AND\\_FAULT\\_STATISTICS\\_2010.pdf](https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/RG_SOC_Nordic/110831_NORDIC_GRID_DISTURBANCE_AND_FAULT_STATISTICS_2010.pdf).
- [16] J. Driesen and F. Katiraei, “Design for distributed energy resources,” *IEEE Power and Energy Magazine*, vol. 6, no. 3, pp. 30–40, 2008.
- [17] H. Jiayi, J. Chuanwen, and X. Rong, “A review on distributed energy resources and MicroGrid,” *Renewable and Sustainable Energy Reviews*, vol. 12, no. 9, pp. 2472–2483, Dec. 2008.
- [18] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Trans. Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Mar. 2004.
- [19] P. E. Heegaard and K. S. Trivedi, “Network survivability modeling,” *Computer Networks*, vol. 53, no. 8, pp. 1215–1234, 2009.

---

# How to Use Mobile Communication in Critical Infrastructures: A Dependability Analysis

Jonas Wäfler and Poul E. Heegaard  
In Floor Koornneef, Coen van Gulijk (Eds.), *Lecture Notes in Computer Science:  
Vol. 9338. Computer Safety, Reliability, and Security*,  
Springer, 2015

© 2015, Springer International Publishing Switzerland.  
Reprinted with permission.





# How to use Mobile Communication in Critical Infrastructures: a Dependability Analysis

Jonas Wäfler and Poul E. Heegaard

Norwegian University of Science and Technology  
N-7491 Trondheim, Norway  
{Jonas.Waefler, Poul.Heegaard}@item.ntnu.no

**Abstract.** Critical infrastructures, like the future power grid, rely strongly on a reliable communication infrastructure. Mobile communication seems an attractive candidate, as the entry costs are low and, provided the coverage, the new devices have immediate communication access upon installation. However, considering the long time-frame of this investment, it is important to think about the constraints in mobile networks and also potential challenges waiting in the future. In this study, which is based on the situation in Norway, we discuss four important future challenges: policy change, contract change, change of *Quality of Service* and network failure. We show that a clever use of mobile communication like multihoming or using a mobile virtual network operator may meet the challenges. In the second part, we quantify the availability of the different mobile communication usages with the help of analytical models and show that already a small increase of additional battery capacity in the mobile network improves the availability significantly.

## 1 Introduction

Like other critical infrastructures, the future power grid is going to rely strongly on a reliable communication infrastructure. Intelligent electronic devices (IED) are going to be deployed throughout the power grid and are in need of a flexible communication platform [1]. The requirements concerning latency, availability and security [2, 3] are very diverse and might be covered by either a flexible middleware framework for data communication like GridStat [4] or a mixture of different technologies. Among the considered technologies, mobile communication is regarded as a pragmatic choice for services like smart metering and monitoring in remote locations. It is a tempting candidate, because the entry costs are relatively low and, provided adequate coverage, the device has immediate communication access upon installation. However, there are many pitfalls to avoid, not least because of the long term nature of the investment.

The mobile networks conduct an access control based on the mobile device's subscription. A device is usually only allowed to use the network of the operator, which issued the subscription. National roaming, i.e. the communication over networks of other operators, is technically possible but commonly not permitted. There are exceptions for special numbers like police and fire department and

for special groups of customers, e.g. in Norway the regulator stipulated national roaming for a limited set of prioritized customers from rescue organizations [5]. If a utility wants to use a different operator because the reception has deteriorated or it changed the contract, it has to manually exchange the SIM card in the device, which may be very costly as the potential number of devices for smart metering and monitoring is very large.

An important property for the suitability of a communication infrastructure is its dependability. Only few public studies exist [6–8] as the access to data is usually restricted. The first two studies focus on operator internal incidents, the third one [8], however, takes a different approach: it is based on measurements done by mobile devices distributed over 300 different places in whole Norway. The logged connectivity to the different UMTS networks show the distribution of time between failures, down time and unavailability. This study measures the Quality of Service exactly how a user would perceive it.

In this paper we suggest several alternatives on how a power utility may use mobile communication; we single out the four main future challenges and analyze how the alternatives react to those. After this qualitative analysis we analyze the availability of the alternatives quantitatively based on measurement data from the study from [8]. And finally, we analyze the availability improvement when equipping the base stations in the mobile network with more battery capacity.

## 2 System Description

We consider the case, in which a company wants to roll-out a large number of mobile devices. These devices could be smart meters or monitoring devices inside the power grid. The study focuses on the implication of using mobile communication for these smart devices, this is done by concentrating on the communication between a single smart device and the company. The mobile communication is provided by two mobile network operators (MNO): *MNO A* and *MNO B*. It is assumed, that there is no national roaming agreement between *MNO A* and *MNO B*, i.e. subscribers of one network have no access to the other network. As in real networks, the two infrastructures are not completely independent and thus their failures manifest some dependencies. The reason is twofold. First, shared infrastructure or geographical collocation of infrastructure in certain parts of the network, e.g. *A* leases a communication line from *B* in rural and sparsely populated areas or *A* and *B* have their cables in the same ditch. Second, dependence on the same service like for example power supply. In both cases one failure can cause a failure in the two MNOs.

The MNOs are considered as black boxes, no internal state is known, the mobile device only knows whether a connection to an MNO is possible and, on a higher network level, if it has a connection to the power utility. It is assumed, that only the MNOs can fail, as they are the main focus of the study.

In order to connect to the mobile network any device needs a SIM card. On each SIM card there is a number (IMSI) which uniquely identifies each device. Part of this number is the mobile network code (MNC), which identifies the



mobile company that issued the SIM card. Access control is based on the MNC, an MNO allows only connections from devices with its own MNC or with an MNC belonging to an MNO with a roaming agreement. In Norway, these roaming agreements are scarce and limited to foreign MNOs or mobile companies owning no or only a very limited network on their own.

## 2.1 Challenges

Any mobile solution faces challenges over its lifetime. In the following we list the challenges, which are in our opinion the most important once.

**Challenge 1: Policy Change** Mobile communication depends on policies from the national regulator and also on policies from the MNO. The national regulator may for example forbid international roaming fees or impose national roaming; the MNO may change national and international roaming agreements.

**Challenge 2: Contract Change** The contract between the subscriber and the MNO is subject to changes over time. Examples are an increase of the subscription fee above an acceptable price level, required services that are discontinued, bankruptcy of the MNO or its acquisition.

**Challenge 3: Change of QoS** The *Quality of Service* (QoS) at a device may change over time. Examples are a reduced signal strength or increased blocking probability because of structural changes between the mobile device and the base station (e.g. new walls, new buildings) or changes in the usage pattern of the base station (e.g. increased number of subscribers).

**Challenge 4: Network failure** A network failure in this context is defined as service outage, i.e. communication from sender to receiver over this specific network is not possible. The mobile device always tries to connect to a base station of its prioritized MNO. If no base station of its prioritized MNO is available, it may try to connect to a base station of another MNO, but a connection is only established if a roaming agreement with that MNO exists.

The time granularity is very different and decreases from the first to the last challenge, i.e. the reaction time for the operator is getting shorter. Policy and contract changes have to be announced with a certain lead time and the operator can look for a solution well in advance. A change of QoS, however, may happen without notice and network failures usually come without warning and the system has to immediately react to mitigate the failure.

## 3 Usage Alternatives

The ordinary way is to buy regular SIM cards from an existing MNO, denoted in the following as *ordinary subscription*. This comes with a carrier lock-in: a change of MNO can only be achieved by replacing the SIM card in each and every device. This is costly, as the number of devices is likely to be high and some of the devices may be located in remote areas or in places difficult to reach. Also a network failure has a strong impact, as a national roaming is usually not allowed, i.e. only the network of your own MNO can be used.

**MVNO** The utility takes the role of a *mobile virtual network operator* (MVNO), buying a certain amount of services from an MNO. Utilities may collaborate nationally to reduce the operational costs.

The MNO can be changed by changing roaming agreements. There are already many MVNOs, so this is a proven solution and it can be implemented quickly by out-sourcing almost everything if desired. A precondition for this solution is that existing MNOs allow roaming by MVNOs. A policy change by the national regulator or the MNOs may therefore have an impact on this solution. An MVNO has usually only an agreement with one MNO and it may happen that no MNO can provide a satisfactory QoS for all the devices. In this case, changing the MNO does not help. This threat is higher for geographically wide spread utilities. In case of a network failure, this solution has the same weakness as the *Ordinary Subscription*, because the network cannot be changed on short notification but needs longer negotiations.

The MVNO may issue several series of SIM cards with different MNCs. It can then make individual roaming agreements for each MNC. This way some of the discussed problems can be mitigated.

**Multihoming** Certain devices allow the use of multiple SIM cards. Using a SIM card from each MNO implements a national roaming without dependencies on policy changes by the regulator or the MNOs. An application on the device probes the different networks and chooses the one with the most favorable QoS. There is a carrier lock-in, however, by using several SIM cards the risk is minimized. Using a SIM card from an MVNO especially for utilities may increase the flexibility of this solution even more. A new MNO can only be used by inserting their SIM card. The cost per device is higher, as it needs multiple SIM card slots and multiple subscriptions per device.

**International Subscription** Interestingly, users with a foreign subscription can have an advantage over those with a national subscription when the foreign MNO has roaming agreements with several national MNOs. In this case, the foreign subscription implements a national roaming.

The advantages are that it is very easy to implement and several mobile networks can be used, depending on the roaming agreements. The switchover to another network may be fast, depending on the network failure. International roaming depends strongly on the policies of the regulator and the MNOs that are in place. If the roaming costs are abolished for good, the MNOs may restrict roaming agreements or make international coalitions with roaming agreements. But all depends strongly on what is defined as legal by the European and the national regulator. Additionally, this solution leads again to a carrier lock-in.

## 4 Unavailability

The availability of the alternatives can be grouped in three classes.

$A_{\text{single}}$ : only one single network is used, if it fails the connection fails as well;

$A_{\text{standby}}$ : there is a standby network, which is used in the case of a failure in the primary one, the switchover time varies between the solutions;

$A_{\text{DMR}}$  (DMR: dual modular redundancy): two networks are used at the same time and a failure in one does not interrupt the connection.

The *ordinary subscription* and *MVNO* (with one MNC) are in the class  $A_{\text{single}}$  because they can only use the network of a single MNC, namely the one having issued the SIM card or the one having a roaming agreement, respectively. The solution *MVNO* (with multiple MNCs) is either in the class  $A_{\text{single}}$  or  $A_{\text{standby}}$ , depending on whether the MNC is fix or whether it can be changed dynamically in case of a network failure. *Multihoming* is in the class  $A_{\text{DMR}}$  if the SIM cards are used in parallel and in class  $A_{\text{standby}}$  if one is in a standby state. The *international subscription* is in the class  $A_{\text{standby}}$  because the device can only be connected to one network at a time and needs to reconnect in the case of a network failure.

We compute the unavailability  $U$  of the classes, given by  $U = 1 - A$ , where  $A$  is the availability defined as “*readiness for correct service*” [9].

#### 4.1 Quantification of $A_{\text{single}}$ and $A_{\text{DMR}}$

The mentioned study [8], contains data for our classes  $A_{\text{single}}$  and  $A_{\text{DMR}}$ . Additionally, it also contains the distributions for *time between failure* and *down time* when using a

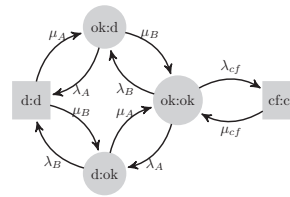
**Table 1.** Used parameters from study [8].  
unavailability failure rate restoration rate

	U	$\lambda_{i,\text{total}}$ [s <sup>-1</sup> ]	$\mu_i$ [s <sup>-1</sup> ]
$A_{\text{single}}$	$3.3 \times 10^{-4}$	$1.11 \times 10^{-5}$	$3.33 \times 10^{-2}$
$A_{\text{single}}$	$5.0 \times 10^{-3}$	$2.01 \times 10^{-6}$	$4 \times 10^{-4}$
$A_{\text{DMR}}$	$2.0 \times 10^{-5}$	–	–

single network. Assuming the distributions to be negative exponential, the failure and restoration rates are computed with the approximated *mean time between failure (MTBF)* and *mean down time (MDT)* by  $\lambda = 1/(\text{MTBF}-\text{MDT})$  and  $\mu = 1/\text{MDT}$ . The parameters are given in Table 1. The two networks have very different properties: *MNO A* has more failures than *MNO B*, but due to its short restoration time it has a lower overall unavailability.

#### 4.2 Quantification of $A_{\text{standby}}$

There are no numbers for  $A_{\text{standby}}$ , however, we show how it can be computed with a Markov model and the given parameters. But first, we note, that the measurements in Table 1 indicate, that *MNO A* and *MNO B* are *not* independent, they are subject to common cause failures. In order to compute this common cause failure rate the Markov model in Fig. 1 is used. The round states are system up states and the square states system down states. The state of the whole system is defined by the states of the two MNOs ( $i_A : i_B$ ) with  $i_A, i_B \in \{\text{ok}, \text{d}, \text{cf}\}$ . The



**Fig. 1.** Model for class  $A_{\text{DMR}}$  with  $i_A, i_B \in \{\text{ok}, \text{d}, \text{cf}\}$ . The

states for each MNO are working (*ok*), down (*d*) or down because of a common cause failure (*cf*). Common cause failures from states other than (*ok:ok*) are omitted for the sake of readability; the introduced error is negligible, as the *ok:ok* state has by far the highest state probability. The  $\lambda_i$ s are computed by  $\lambda_i = \lambda_{i,total} - \lambda_{cf}$  in order to keep the total failure rates  $\lambda_{i,total}$  constant when varying  $\lambda_{cf}$ . Setting  $\lambda_{cf} = 0$ , i.e. making the networks independent, we get an unavailability of  $1.67 \times 10^{-6}$ , i.e. around 12 times smaller than the measured unavailability in Table 1, showing that the networks are in fact dependent as mentioned above.

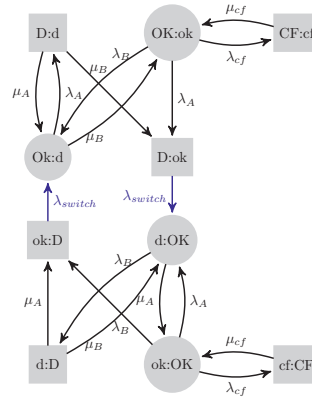
Details about shared infrastructures and services in *MNO A* and *MNO B* are not known. However, leased line and power incidents are possibly large contributors to failures [6], therefore, we assume a restoration time of  $1/\mu_{cf} = 2500s$ , which is in the order of a longer mobile restoration time and a power outage restoration [10]. Solving the model with the unavailability and rates given in Table 1 yields a common cause failure rate  $\lambda_{cf}$  as listed in Table 2. The failure rate  $\lambda_{cf}$  makes around 5% of the total failure rate of *MNO A*  $\lambda_{A,total}$  and around 30% of *MNO B*  $\lambda_{B,total}$ .

Finally, the unavailability for  $A_{standby}$  is computed by extending the state definitions to ( $j_A : j_B$ ) with  $j_A, j_B \in \{ok, OK, d, D, cf, CF\}$ , which yields the model depicted in Fig. 2. Uppercase letters indicate that the mobile device is currently using that network. E.g. state (*ok : D*) means network B is used, but *down* and network A is *ok*. It is a down state (square), only after switching the network, leading to state (*Ok : d*) is the system up and running again.

In a business oriented setting it can be advantageous to prefer one MNO over the other because of special price models based for example on data volume. The other MNO is only used if the preferred one is down. For that, the model in Fig. 2 is adjusted to always switch over to the preferred network if it is working. i.e. if *MNO A* is preferred, adding a new transition from (*ok:OK*) to (*OK:ok*) and marking the former state as down state because of the unavailability during the switchover.

**Table 2.** Common cause rates after parameter fitting.

$$\frac{\lambda_{cf} [s^{-1}]}{6.34 \times 10^{-7}} \quad \frac{\mu_{cf} [s^{-1}]}{4 \times 10^{-4}}$$

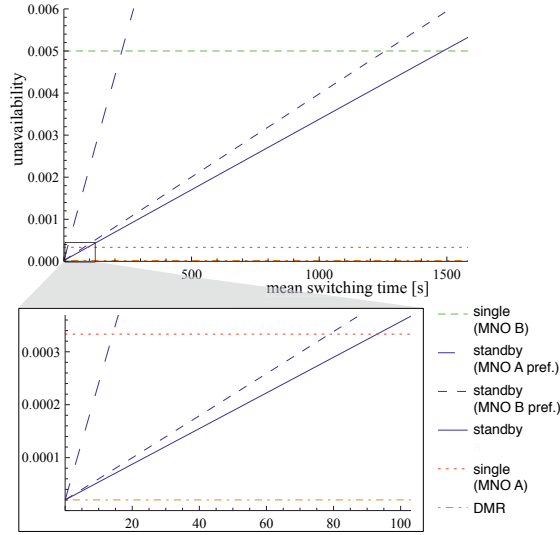


**Fig. 2.** Model for class  $A_{standby}$  to the preferred network if it is working. i.e. if *MNO A* is preferred, adding a new transition from (*ok:OK*) to (*OK:ok*) and marking the former state as down state because of the unavailability during the switchover.

### 4.3 Discussion

The results of a steady-state analysis are given in Fig. 3. They show clearly the large difference in unavailability of the different solutions. Class  $A_{single}$  has two results depending on which MNO is chosen. The difference between the two MNOs is big because of the large difference in restoration time.

In the class  $A_{\text{standby}}$ , the unavailability is linearly increasing with the mean switching time. The unavailability is lower than the unavailability of  $A_{\text{single}}$  if the mean switching time is lower than 95 seconds or 1485 seconds for *MNO A* and *MNO B*, respectively. The first number is surprisingly small, it is explained by the very short average restoration time in *MNO A* of  $1/\mu_A = 30\text{s}$ . The switching time itself depends strongly on the used alternative and implementation. Two alternatives belonging to the class  $A_{\text{standby}}$  may, therefore, not necessarily have the same unavailability.

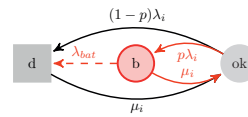


**Fig. 3.** Unavailability of the classes against switching time. Zoom-in for low values of switching time.

Preferring one MNO leads to a higher unavailability. *MNO B* is here the better choice of the two, as this solution benefits from the longer uptime of *MNO B* and the shorter restoration time of *MNO A*. Preferring one MNO creates additional interruptions, i.e. a lower mean time between failure (MTBF) and should be avoided. However, as stated above there might be other considerations that need to be taken into account. We consider the system as down during the switchover, if it is performed without downtime, then preferring *MNO B* has a lower unavailability than the standard standby class.

## 5 Improving Availability with Batteries

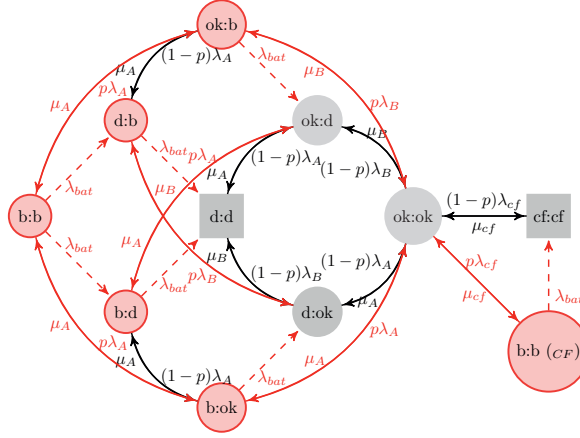
Today, batteries are available in some base stations. Depending on the MNO the number of equipped base stations as well as capacity varies strongly. In Norway there are discussions between the national regulator and MNOs about stipulating a required battery installation in base stations in mobile networks [11]. So far, installed batteries in the power grid were already included implicitly, because we used measurements of actual networks. In the following we study the effect of installing additional battery capacity.



**Fig. 4.** Model for class  $A_{\text{single}}$  with limited battery capacity.

Batteries allow the communication system to keep on working in case of a power failure, if it is bridgeable by battery. We assume that this is the case for  $p\%$  of all failures, valid for both individual failures and common cause failures. The battery capacity is assumed to be negative exponentially distributed with mean  $1/\lambda_{\text{bat}}$ . This assumption is justified by the variation of capacity due to different battery types, battery ages, working conditions and charging states.

The extended models for the classes  $A_{\text{single}}$  and  $A_{\text{DMR}}$  are depicted in Fig. 4 and Fig. 5. The state definition is extended by the network state  $b$ , indicating that the network suffered a power failure and parts of it is running on battery. The dashed arrows indicate a transition caused by battery depletion. The model for  $A_{\text{standby}}$  is not depicted but is constructed as before



**Fig. 5.** Model for the class  $A_{\text{DMR}}$  with limited battery capacity.

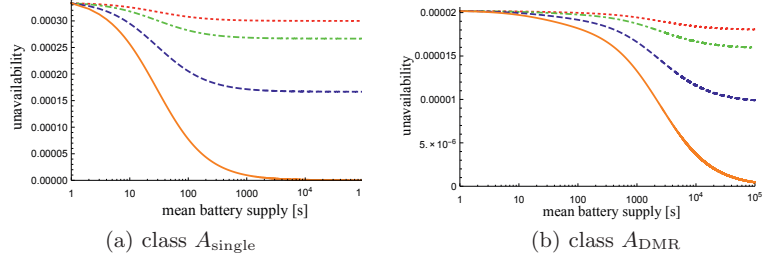
by duplicating the model for  $A_{\text{DMR}}$ , adding an indication for which MNO is active and adding two new transitions with rate  $\lambda_{\text{switch}}$  between  $ok:D$  to  $OK:d$  and  $D:ok$  to  $d:OK$ .

## 5.1 Discussion

Fig. 6(a) shows the results for the class  $A_{\text{single}}$  when using *MNO A*. The unavailability is most sensitive to a mean battery capacity in the order of the mean down time, i.e.  $1/\mu_A = 30$  seconds. For the *MNO B* the plot would look similar, but shifted towards its mean down time of  $1/\mu_B = 2500$  seconds.

Fig. 6(b) shows the results for the class  $A_{\text{DMR}}$ . The two parameters  $\lambda_{\text{cf}}$  and  $\mu_{\text{cf}}$  are set to the values used previously, noted in Table 2, which equals to a mean *common cause restoration time* of 2500 seconds. As expected are the absolute values lower than in the class  $A_{\text{single}}$ ; the plot is in fact almost the same as for *MNO B*, except the y values are much lower. The reason being, that of the two down states in the model, the state  $cf:cf$  is responsible for the highest fraction of the down time. The mean sojourn time for this state is given by  $1/\lambda_{\text{cf}}$  and is equal to the restoration time in *MNO B*.

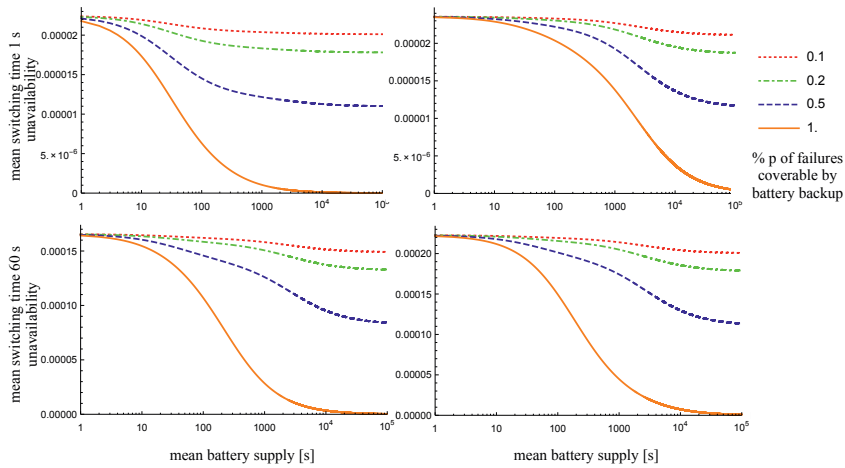
Fig. 7 shows the results for the class  $A_{\text{standby}}$ . The simulation is done for two scenarios with different pairs for  $\lambda_{\text{cf}}$  and  $\mu_{\text{cf}}$ . In scenario 1,  $1/\mu_{\text{cf}}$  is chosen to be very short, i.e. 30 seconds, which corresponds to the restoration rate of *MNO A*. As before,  $\lambda_{\text{cf}}$  is given indirectly by the model in Fig. 1 by solving the steady



**Fig. 6.** Unavailability against battery capacity for different values of  $p$ .

state equations for it. In scenario 2, the two parameters  $\lambda_{cf}$  and  $\mu_{cf}$  are set to the values used previously, i.e.  $1/\mu_{cf}$  of 2500 seconds. Additionally, it is done for two different switching times. For a switching time of 1 second the difference between the two scenarios is big, i.e. the downtime caused by the common cause failure is dominant. When increasing the switching time to 60 seconds, however, the downtime caused by the switching itself becomes dominant and the difference between the two scenarios is minimal.

The numbers show that the availability gain can already be large for a small battery capacity bridging a time of 1-3 minutes. However, it depends strongly on the restoration times and switching times between the networks.



**Fig. 7.** Unavailability against battery capacity for class  $A_{standby}$  with different values of  $p$ . Left column uses  $1/\mu_{cf} = 30s$ , right column  $1/\mu_{cf} = 2500s$ .

## 6 Conclusion

We list different alternatives of how to use mobile communication in this paper. By combining them, more are possible, but they are not fundamentally different to the presented ones. As the machine-to-machine communication (M2M) is likely to increase in the future, new technologies and especially new regulations may change the way mobile communication is used. For example, a decoupling of the SIM card and the operator by issuing carrier-free SIM cards would allow the switching between different networks and subscription contracts with only a short switching delay. This would inexpensively implement a virtual multihoming belonging to the availability class  $A_{\text{standby}}$  as discussed above.

This study is based on the regulation status and availability statistics in Norway. Details might be different in other countries. If and how mobile communication should be used depends on what service is run over it and its requirements concerning availability, performance and costs. In this paper we only focused on future challenges, usage alternatives and the availability; performance and costs are important factors but were outside the scope.

## References

1. International Energy Agency (IEA), “Technology roadmap: Smart grids,” 2011.
2. D. E. Bakken, A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle, “Smart generation and transmission with coherent, Real-Time data,” *Proceedings of the IEEE*, vol. 99, no. 6, pp. 928–951, Jun. 2011.
3. Electric Power Research Institute (EPRI), “The integrated energy and communication systems architecture, volume IV: Technical analysis,” Tech. Rep., 2004.
4. H. Gjermundrod, D. E. Bakken, C. H. Hauser, and A. Bose, “GridStat: a flexible QoS-Managed data dissemination framework for the power grid,” *IEEE Transactions on Power Delivery*, vol. 24, no. 1, pp. 136–143, Jan. 2009.
5. “Forskrift om prioritet i mobilnett,” [Regulation about Priorities in Mobile Networks], FOR-2013-10-21-1241, NKOM, Norwegian Communication Authority, October 2013.
6. E. L. Følstad and B. E. Helvik, “Failures and changes in cellular access networks; a study of field data,” in *Proc. DRCN*, 2011, pp. 132–139.
7. S. M. Matz, L. G. Votta, and M. Malkawi, “Analysis of failure and recovery rates in a wireless telecommunications system,” in *Proc. Dependable Systems and Networks (DSN)*, 2002, pp. 687–693.
8. A. Kvalbein, “Robusthet i norske mobilnett,” [Robustness in Norwegian mobile networks], simula research laboratory, Tech. Rep., 2013.
9. A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Trans. Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, Mar. 2004.
10. “Avbrottsstatistikk 2013,” [Outage statistics 2013], NVE, Norwegian Water Resources and Energy Directorate, November 2014.
11. “Sikkerhet og beredskap mot ekstremvær i telesektoren,” [Security and preparedness for extreme weather situations in the telecommunication sector], Working Group Energi Norge and Telenor, Tech. Rep., 2013.



---

# Interdependency in Smart Grid Recovery

Jonas Wäfler and Poul E. Heegaard

*Proc. Reliable Networks Design and Modeling (RNDM)*, Munich, Germany,  
Oct. 2015

© 2015, IEEE. Reprinted with permission.





# Interdependency in Smart Grid Recovery

Jonas Wäfler and Poul E. Heegaard  
Department of Telematics  
Norwegian University of Science and Technology  
N-7491 Trondheim, Norway  
{jonas.waefler, poul.heegaard}@item.ntnu.no

**Abstract**—The pervasive use of information and communication technology (ICT) in the future power grid creates an interdependent system: ICT systems depend on power supply and the power grid depends on information channels and systems for monitoring and controlling. The automation of processes with ICT can reduce the most frequent failures and decrease their consequences. However, the added complexity and the tight integration comes with new failure sources and increased mutual dependencies between the systems and opens the possibility for more catastrophic failures. In this paper we focus on these interdependencies between the power grid and ICT in different phases of the recovery process of a power failure. We model the dependencies and quantify the effect of using smart monitoring devices in the detection phase. The analysis shows that adding battery backup into the communication network is a good measure to delay the interdependency effect encountered. The study of scenarios with different degrees of battery support, number of repair crews and fault detection mechanisms indicates that while automation can reduce the human effort needed for the most frequent failures, it can lead to longer down times in less frequent incidents, if no prevention measures are taken. Finally, we show that the skill sets and training level of the repair crews play a crucial role and can be used to prevent the negative effect in low frequency incidents.

## I. INTRODUCTION

The today's power grid depends on functioning information and communication technology (ICT) services for various aspects like monitoring, controlling and protection. In the future power grid, the smart grid, this dependency is expected to increase even more [1]. What makes the relation between the power grid and the supporting ICT complex, is that on one side the power grid relies on the ICT to get data and to control the system, but on the other side, the ICT system needs the power grid for power supply. Hence, we have an interdependent system [2], [3]. In order to understand such a system, it is crucial to investigate both of the systems and their interactions [4]–[6].

Studies of major power grid incidents show the importance of these interdependency effects in the past [7]–[9]. A formalism to classify the different types of interdependencies and failures is put forward in [2] and there are theoretic results focusing on a long chain of failures cascading back and forth between the power grid and the ICT system [7].

The introduction of new services based on ICT comes also with the potential to increase the dependability of the power grid [10]. The promise is that the automation of processes can reduce the most frequent failures, which can be called the primary effect. However, the new systems contain more

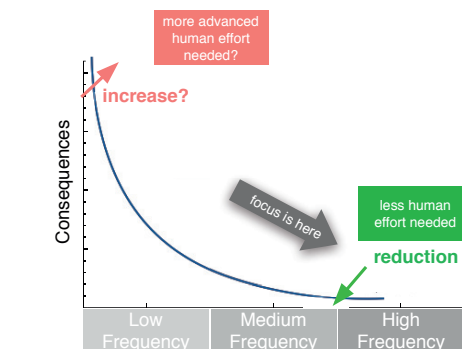


Fig. 1: Schematic example how the introduction of automation may influence the risk curve of a system.

sophisticated software and more configuration possibilities. This makes the development, configuration and maintenance more critical and complex. Let's call this the secondary effect. Two large studies on the public switched network and critical infrastructures showed that the majority of failures are either human made due to wrong maintenance, configuration or accidents [11]; or software related [12]. Human made failures may be caused among others by the complexity of large networks with its various technical concepts, historically grown solutions, and its continuous renewal of technology [13].

The mentioned primary and secondary effects of the introduction of ICT can be visualised in a simple plot as shown in Fig. 1. The hyperbola represents the risk curve of a specific system. The focus is usually on the primary effect of the ICT support, which is supposed to reduce the frequency and the consequences of high frequency incidents, denoted by the arrow on the right side. The automation reduces human effort for these incidents. However, there is also a change on the other end of the scale, caused by the secondary effect. Without any prevention this can lead to larger consequences in low frequency incidents.

A situation where the interdependency between power grid and ICT becomes apparent is during the recovery of a power grid incident. The repair crews have a need to communicate with the control centre but the prevailing failure in the power grid has an influence on the power supply of the commu-

nication system and its availability. Norway, a country with remote regions and harsh weather conditions, suffered several large winter storms in the last years. The power outages were followed by the outage of the mobile network, which then slowed down and impeded the recovery process. Triggered by this events, the national regulator and the mobile network operators (MNOs) started the discussion about stipulating a required minimal battery supply in parts of the mobile networks [14], which would delay the dependency effect on the communication system.

In this paper, we focus on the interdependency in the smart grid during the recovery process. We take a survivability approach in which the study starts the moment the system fails and ends with its full recovery [15]. The recovery process is split into several phases and the interdependencies between power grid and ICT systems are analysed step-wise for all of them. Based on this, we propose an analytical model for the recovery phase. First, it is used to investigate the potential of automation and additional battery supply in the communication network to delay the interdependency effects between the systems. Second, it is used to analyse scenarios with different degrees of battery support, automation and number of repair crews, under high, medium and low frequency incidents. Finally, we discuss the impact of automation on the needed skill set for the repair crews and its implications for the recovery time.

## II. PROBLEM DESCRIPTION

The objective is to model the interdependency between the power grid and the communication network during recovery. More precisely, we are interested in the case, in which the power grid suffers an outage that needs a repair crew to go on location to conduct a repair. The repair crew is using mobile handsets to coordinate among each others and with the operator at the control centre. For operation, however, the mobile network relies on the power supply by the power network. The most critical components in the access network of the mobile network are the base stations. While on place for the repairing activity, the handsets of the repair crews are connected to the base stations in the area affected by the outage. Most important, the base stations, to which the mobile handsets connect to, are in the same region as the power incident and are likely to be affected by the power outage. The base station may have an uninterruptible power supply (UPS) in form of a battery pack, which allows staying operable for a certain time after the power went out. As soon as the base station becomes unpowered, the mobile communication in that specific region is not possible anymore and the repair crew is slowed down because it has to work without communication. Note, in highly populated areas there are usually several base stations within reach. For this paper, we consider a sparsely populated area with a low density of base stations as it is found in large parts of Norway.

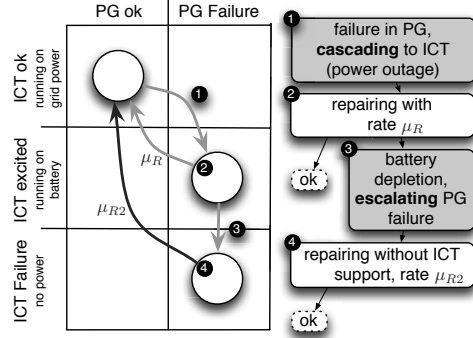


Fig. 2: State diagram showing the cascading and escalating interdependency failures during a power failure and its restoration, with  $\mu_R > \mu_{R2}$ .

### A. Dependencies between Power Grid and ICT

The dependencies in this system are two-fold. First, the communication system depends on the power grid for power supply. Second, the length of the recovery process depends on the correct operation of the communication system.

The high-level state diagram in Fig. 2 shows the dependencies in the failure case in more details. The model is drawn along the two axes showing the state of the power grid (PG) and the communication system (ICT) as described in [6]. The failure in the power grid leads to a power outage in the base station, which transitions into an excited state, because it is now running on a finite battery supply. If no battery was available, it would go straight into a failed state. This is categorized as a cascading failure according to [2], meaning the power failure is the single cause why the ICT system transitions into an excited or failed state. The power grid is now being restored, however, if the battery supply runs out before its completion, the loss of communication leads to a slower restoration rate. This mechanism is categorized as escalating failure according to [2], meaning the power grid is already in a critical or failed state but is additionally negatively affected by the state change of another system, i.e. the failure in the communication system.

### B. Dependencies inside the Power Grid

There are additional dependencies, which concern only one system. In a hurricane situation the probability is high that several lines or stations in the power grid suffer a failure at the same time. This leads to a state in which the repair staff becomes a scarce resource and the repair of a failure needs to be delayed until the necessary resources are available. The recovery time for a failure depends, therefore, on the availability of resources or more general on the state of the rest of the power grid. This dependency can be seen as a failure escalation as the failure in part of the system is escalated, i.e. the recovery time is increased, if the repair crews are already busy repairing other failures.

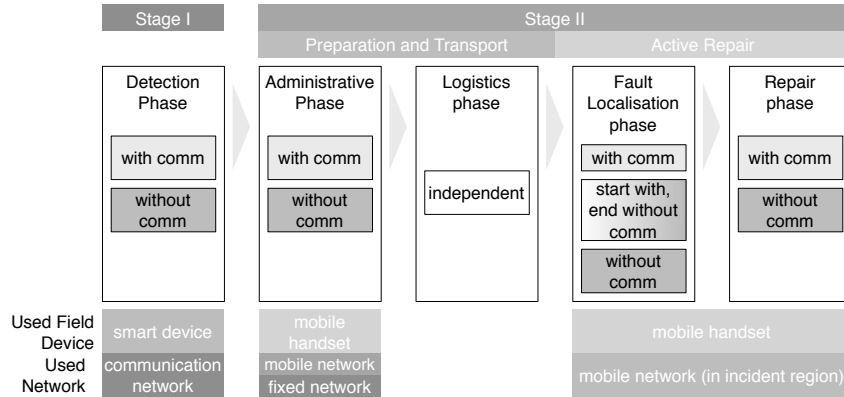


Fig. 3: Recovery stages of the phased recovery from a power grid incident (phases are based on ITU-T E.800 (1994) [16]).

### III. RECOVERY

The recovery process is split into the different phases based on the partitioning of the down time as described in ITU-T E.800 (1994) [16]. The phases are depicted in Fig. 3.

#### A. Recovery Stages

There are five phases in the recovery process:

- **Detection phase:** This phase comprises the detection delay between the moment a failure happens until it is actually noticed in the monitoring system and the time to gather information about the incident. The power grid is equipped with a protection system and fuses, which work independently. Without monitoring devices installed, the incident is not reported directly to the control centre. Depending on the size of the incident, the control centre may indirectly notice it by a load drop or other indications. Monitoring devices throughout the system can detect failures close to real-time and thereby reduce the detection time drastically. The level of details known about the incident can vary from knowing the location, affected components and exact fault type to basically nothing. However, the system relies on a communication channel between the devices and the control centre and on power for the devices. The devices need only a short time span in the order of seconds to collect data about the incident and inform the control centre.
- **Administrative phase:** The recovery is planned and the repair crew has to be assigned and instructed. This includes using a communication system to reach the repair crew, which might be located in a different region or might be on duty in the field. The used network is either a fixed network or a mobile network, depending on the location of the crew.
- **Logistics phase:** The repair crew is gathering the needed material and equipment and drives to the location of the incident.

- **Fault localisation:** This phase includes the precise geographical location and finding the cause of the failure. This may include communication with the control centre to get additional information about the system or the failed devices. This is especially important for less trained or inexperienced workforce.
- **Repair phase:** The system is repaired and brought back to normal operation.

#### B. Role of Communication

The used communication devices and communication networks change over the phases. In the detection phase smart monitoring devices are used, which are distributed over the whole network. They use a communication network that can either be the utilities own network or a public network. All the following phases use only mobile handsets as field devices. The used network is the mobile network but the region in which it is used changes. In the administrative phase the mobile handsets are used quite probably outside of the region where the incident happened. In the logistics phase the repair crew is relocating itself towards that region and for the last two phases they are in the exact location of the incident. The base stations in the access network of the mobile network in this specific location depends on power supply and is suspect to a failure if no battery power backup is available.

As explained above, the importance of information from the field devices and a working communication channel is different in the recovery phases and influence the sojourn time for the phases. This is illustrated in Fig. 3 with the boxes inside the phases.

- **Detection phase:** The sojourn time depends on the existence of monitoring devices and an available communication channel to the control centre. If both are provided, the sojourn time is in the order of seconds, if not, it is in the order of several minutes and up to hours.
- **Administrative phase:** The sojourn time in the administrative phase is in the order of several minutes if the

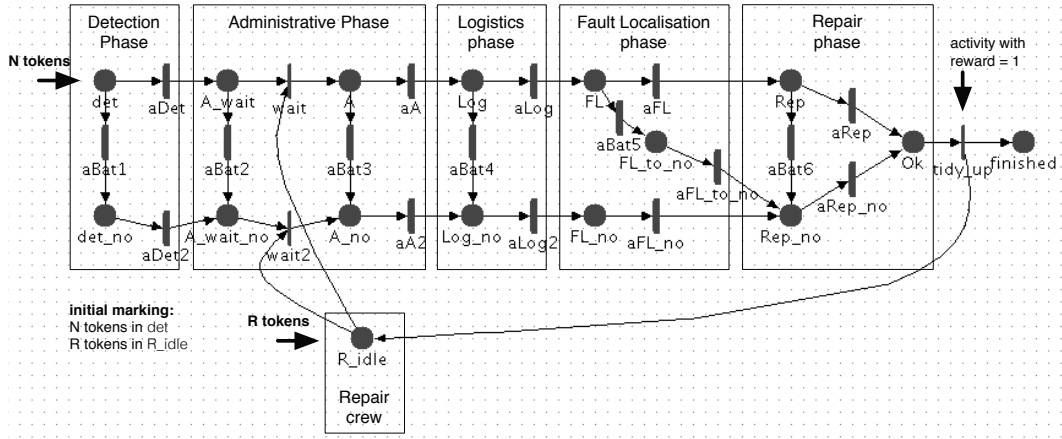


Fig. 4: Stochastic activity network for the recovery phases (print screen from the Möbius tool [17]).

communication system is working and in the order of hours if it is not working.

- Logistics phase: This phase is dominated by the transportation time and is modelled as independent from the availability of a communication system. Any communication activity is moved to the administrative phase. Its sojourn time is in the order of tens of minutes to hours.
- Fault Localisation phase: The sojourn time depends on the availability of the communication system to get additional information about the system or the failed device. Additionally, it depends on the detection phase. If the detection came from a smart monitoring device, then the precise location and problem is known and the needed time is short, i.e. in the order of tens of minutes. There is a third case in this phase, namely when the communication dies while the phase is ongoing. The repair crew may have received already certain information from the control centre and the sojourn time is shortened compared to the case without communication from the beginning but is longer than the case with communication. The sojourn times are in the order of tens of minutes.
- Repair phase: The sojourn time depends also on communication as the recovery of the system can happen smoother when communicating with the control centre. The times are in the order of tens of minutes.

### C. Model

The system is modelled with a stochastic activity network (SAN) [18]. The cases *detection with communication* and *detection without communication* are not in the model, but are distinguished by using a different set of intensities in the model. We assume that the fixed network is used for communication in the administrative phase and, for the sake of simplicity, we assume that this does not fail.

The model is depicted in Fig. 4. The places are mirrored into a second row representing the state in which the batteries in the base stations in the incident regions are depleted. Therefore, the fault localisation and the repair phase cannot use mobile communication. It is important to note, that this gives no information about the availability of the communication in the other phases. This modelling decision is taken to allow analysing multiple failures in the same model by simply increasing the number of tokens in the initial marking.

Stage I of the recovery, i.e. the detection phase, runs independent of repair crews, but as soon as Stage II is entered, the recovery process is stopped until a repair crew is available. This is modelled with a place representing the pool of available repair crews, the consumption of one token from that place at the start of Stage II and setting back a token after finishing the recovery.

The initial marking is  $N$  tokens in the place  $det$  and  $R$  tokens on  $R\_idle$ , where  $N$  is the number of failures in the system and  $R$  the number of repair crews. The timed activities, represented by a thick bar, follow all exponential distributions and are multiplied by the number of tokens in the respective input place to allow modelling multiple failures. The thinner bars ( $wait$ ,  $wait2$ ,  $tidy\_up$ ) represent instantaneous activities firing as soon as all input places contain a token. These transitions are introduced to make the model easier to read.

### D. Numerical analysis

We first analyse the model numerically for a single failure, i.e.  $N = 1$ , using the rates as given in the first two columns of Table I for the activities. The numbers are based on data for longer outages from the Norwegian regulator [19]. In 2013 the mean down time (called CAIDI in power engineering) was 1.36 hours.

TABLE I: Rates used in the numerical analysis.

activities	detection mechanism		
	automatic [min <sup>-1</sup> ]	manual (1) [min <sup>-1</sup> ]	manual (2) [min <sup>-1</sup> ]
aDet, aDet2	1/1	1/20	1/20
aA, aA2		1/5	1/5
aLog, aLog2		1/15	1/15
aFL	1/10	1/20	1/30
aFL_to_no	1/15	1/30	1/45
aFL_no	1/22	1/45	1/90
aRep		1/10	1/15
aRep_no		1/15	1/30
aBatr, $x \in \{1, 2, 3, 4, 5, 6\}$	1/(battery supply)		

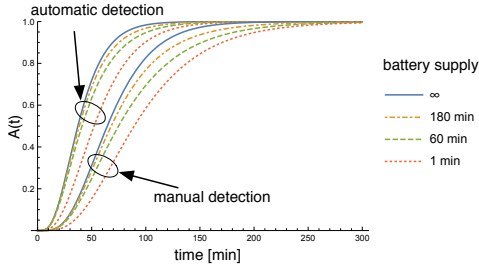


Fig. 5: Instantaneous availability  $A(t)$  during the recovery process.

The quantitative analysis of the SAN is done by simulation runs with the Möbius tool [17]. The results are mean values of 10'000 simulation runs for each parameter set.

For the first analysis, an impulse reward is added to the very last transition in the SAN model called `tidy_up`. Whenever this transition fires, a reward of 1 is given. The time distribution of this reward gives the distribution of the recovery time. The cumulative distribution function (CDF) is then equal to the instantaneous availability during recovery:  $A(t) = P(T_{\text{recovery}} \leq t)$ , which also denotes the probability that the recovery time  $T_{\text{recovery}}$  is less than  $t$ .

The result is given in Fig. 5. The lower four curves show the results for manual detection, the upper four curves the result for automatic detection. Both, having an automatic detection and having a battery supply at the base stations have a positive effect on the recovery speed.

In order to break down the effect on the different recovery phases, we repeat the simulation with a different reward function. A reward of 1 is given after leaving any of the five recovery phases. The rewards are then summed up over time and the results are plotted in Fig. 6. The plot shows how the battery supply influences the availability only after entering the later recovery phases. The automatic detection has the strongest impact in the first phase and in the fault localisation phase.

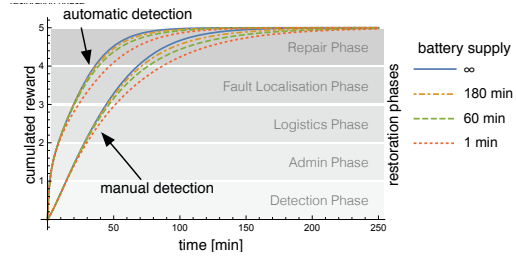


Fig. 6: Expected recovery phase at a given time  $t$ .

### E. Costs

The installation of additional battery has a clear effect on the recovery process, however, it comes with an installation and maintenance cost. In Norway there are discussions between the regulator and the mobile network providers to increase the battery supply in the network [14]. On the other side, there are costs for the power utility during the recovery process for the smart monitoring devices, material, equipment and the repair crews. Increasing battery supply increases both the dependability of the network and the costs for the society. For a utility under pressure it might be tempting to reduce recovery costs by profiting from the battery supply in the mobile network by reducing the number of repair crews. The impact of this reduction is analysed in the next section.

In our analysis we do not consider cost in more details, it is outside the scope of this paper. But the main point is, that the expenses are on the mobile operators, while the potential savings are for the power utilities.

## IV. RISK CURVE

### A. Consequence of Incident

The risks of a system are analysed by studying the probability or frequency of an incident and its consequences. The analysis yields a characteristic risk curve for a system. As a measure for the consequence we use the mean down time (MDT) of a system. It is computed by getting the recovery distribution, i.e. the instantaneous unavailability  $U(t) = 1 - A(t)$  beginning immediately after a failure, where  $A(t)$  denotes the availability. The MDT is now computed by integrating  $U(t)$  over time

$$\text{MDT} = \int_0^{\infty} U(t)dt = \int_0^{\infty} 1 - A(t)dt$$

Another option for the measure is the cost of energy not supplied (CENS), which is used in the Norwegian regulation framework [20]. It also uses the down time for the calculations but includes more information like the estimated costs of an outage for a specific customer group. For the sake of simplicity, we only concentrate on the down time as a measure because it is the dominating factor.

A power utility may profit from battery supply in the mobile network by decreasing the number of repair crews, which

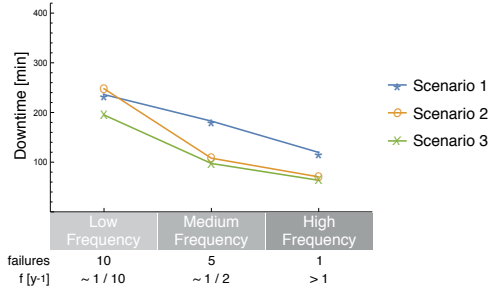


Fig. 7: Mean Down Time (MDT) for the scenarios under the three incidents.

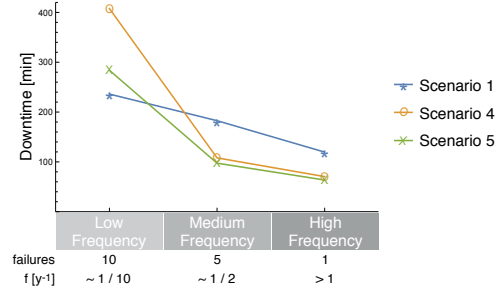


Fig. 8: Mean Down Time (MDT) for the scenarios under the three incidents.

leads to a cost cut. Table II shows a simple comparison of a system having no battery, and a system having an average of 180 minutes battery supply and a decreasing number of repair crews. There are 5 failures in each of the systems.

The MDTs show clearly the effect of the battery supply. When having no battery supply, the MDT with 5 repair crews is slightly longer than the MDT with 180 minutes battery supply but only two repair crews. However, these results are only valid for 5 failures in the system. A system needs to be analysed over a range of different incidents before a decision about a reduction of repair crews can be taken.

#### B. Considered Incidents

We compute the risk curve for our system for the following three different incidents:

- *high frequency incident*: Incident happening several times a year. We use a single power grid failure.
- *medium frequency incident*: Incident happening every other year, like a smaller storm leading to several power grid failures. In the numerical example we use 5 failures.
- *low frequency incident*: Incident happening once in 10 years, like a hurricane that causes a larger number of power grid failures. In the numerical example we use 10 failures.

#### C. Numerical analysis

We consider several scenarios for the system and start with the top three rows in Table III. Scenario 1 is the old system. There are no monitoring devices in the network and the detection phase is, therefore, manual. There is no battery supply for the base stations. The used parameters are listed in

TABLE II: Influence of reducing repair crews when having battery supply.

Failures	Repair Crews	Battery [min]	MDT [min]
5	5	0	106
5	5	180	76
5	2	180	101
5	1	180	144

Table I, in the column *manual (1)*. Scenarios 2 and 3 both have some battery supply but a reduced number of repair crews. They also have smart devices that provide an automatic detection in the high and medium frequency incident case. In the low frequency incident, i.e. the rare event, it is assumed that the communication to this devices is cut and that the detection has to happen manual as well. The used parameters are listed in Table I, in the columns *manual (1)* and *automatic*.

#### D. Missing Training and Practise

In the previous case it is implicitly assumed that the repair crews in Scenario 2 and 3 manage the recovery phases in the low frequency incidents with the same efficiency as the repair crews in scenario 1. However, this might be unrealistic as they most often operate with information sent to them from the smart devices during the automatic detection. Only seldom do they perform a recovery starting with a manual detection. Therefore, there might be less operational knowledge, less training and missing skills for the recovery phases without the information from the smart devices. In addition, a repair crew in the automatic detection case does not need the same knowledge and background as one in scenario 1, which might have an effect on the staffing. The combination of these reasons, leads to the conclusion, that the repair crews might perform worse in the low frequency incident than the repair crews in scenario 1, and the results are probably too optimistic. Therefore, we create the scenarios 4 and 5, which are replicas of scenarios 2 and 3, but with adjusted rates. The scenarios are given in Table III and the parameters in Table I in the columns *manual (2)* and *automatic*. For the parameters in *manual (2)*, the expected activity time in *manual (1)* are multiplied by 1.5

TABLE III: Scenarios (parameters are given in Table I).

Scenario	Battery [min]	Repair Crews	Detection in incident case:		
			Low	Medium	High
Scenario 1	0	5	manual (1)		
Scenario 2	30	3	manual (1)	automatic	
Scenario 3	180	3	manual (1)	automatic	
Scenario 4	30	3	manual (2)	automatic	
Scenario 5	180	3	manual (2)	automatic	



if the communication to the control centre still is available and by 2.0 if the communication is not available.

#### E. Discussion

The results are shown in Fig. 7 and Fig. 8. They show, that the scenarios 2, 3, 4 and 5 have a significant lower MDT than scenario 1 for high and medium frequency incidents, even though they use less repair crews. The reason is two-fold. First, the battery supply, which delays the power outage in the communication network allows the repair crews to communicate with the control centre and reduces the recovery time. Second, the automatic detection with the smart monitoring devices gives valuable information about the exact place and nature of the failure. In other words, the advantage of the introduction of monitoring devices, and strengthening of the communication platform, is so strong that it is even possible to downsize the number of repair crews and still have a better performance, i.e. a lower MDT, than without.

However, in incidents with lower frequency, the improvements have the opposite effect. The scenario 2 and 3 perform here similar to scenario 1, which has no battery supply at all. The scenarios 4 and 5 have a more pronounced risk curve and the MDT is actually higher than in scenario 1.

The results indicate, that decreasing the consequences of the most common incidents by increasing the automation and using less trained employees can have the inverse effect in rare events. This can be circumvented by the following endeavours. First, by not downsizing the repair staff. Second, by keeping the repair staff on a high training standard and having efficient and well-established processes for the rare events. However, the utilities are under a certain economical pressure and the incidents in which the additional repair staff or the additional skills are needed are seldom. Therefore, this might be overlooked or ignored to save money. As both the MNOs and the power utilities are regulated, the pressure might also come from the regulators to counterbalance the investment costs for the battery supply on a macro-economic level. Hiring repair staff on demand might help, but there the risk of missing training and practise is even more noticeable and in a critical situation the skilled repair staff might be a scarce resource.

An additional option is to compensate the reduction of repair crews and the change of skill sets by employing additional specialist that can cover the rare events as indicated in Fig. 1.

#### V. CONCLUDING REMARKS

One of the characteristics of the smart grid is the wide use of ICT to operate the power grid more efficient and in a more reliable way. The automation of processes reduces the most common failures and makes them less severe. However, the added complexity and the tight integration comes with new failure sources and increased mutual dependencies between the systems. We focused on modelling and analysing these interdependencies between the power grid and the communication system in the different phases of the recovery process.

As shown in this paper, it is possible to reduce or delay the dependency by adding battery supply to the most critical part

of the mobile network and adjust the skill sets of the repair staff to cover not only the most frequent failures, but also the rare events in which deep knowledge about the system is necessary.

There are costs for minimising and preventing failures, but also for the recovery of failures. They have to be balanced by either the market or legislations from the regulator. We touched upon it very briefly but in general, it is outside the scope of this paper.

#### REFERENCES

- [1] International Energy Agency (IEA), "Technology roadmap: Smart grids," [www.iea.org/publications/freepublications/publication/smartgrids\\_roadmap.pdf](http://www.iea.org/publications/freepublications/publication/smartgrids_roadmap.pdf), 2011.
- [2] S. Rinaldi *et al.*, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, Dec. 2001.
- [3] M. Amin, "National infrastructure as complex interactive networks," in *Automation, control and complexity*, T. Samad and J. Weyrauch, Eds. New York, USA: Wiley, 2000, pp. 263–286.
- [4] D. Kirschen and F. Bouffard, "Keeping the lights on and the information flowing," *IEEE Power and Energy Magazine*, vol. 7, no. 1, pp. 50–60, Jan. 2009.
- [5] J.-C. Laprie *et al.*, "Modelling interdependencies between the electricity and information infrastructures," in *Proc. SAFECOMP, Nuremberg, Germany*, 2007, pp. 54–67.
- [6] J. Wäfler and P. E. Heegaard, "Interdependency modeling in smart grid and the influence of ict on dependability," *Advances in Communication Networking, 19th EUNICE/IFIP WG 6.6 International Workshop, Chemnitz, Germany*, pp. 185–196, August 2013.
- [7] S. V. Buldyrev *et al.*, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.
- [8] G. Andersson *et al.*, "Causes of the 2003 major grid blackouts in north america and europe, and recommended means to improve system dynamic performance," *IEEE Trans. Power Syst.*, vol. 20, no. 4, pp. 1922–1928, Nov. 2005.
- [9] Z. Xie *et al.*, "An information architecture for future power systems and its reliability analysis," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 857–863, Aug. 2002.
- [10] V. V. Vadlamudi *et al.*, "Challenges in smart grid reliability studies," in *Proc. 12th Int. Conf. on Probabilistic Methods Applied to Power Systems (PMAFS), Istanbul, Turkey*, June 2012.
- [11] D. Kuhn, "Sources of failure in the public switched telephone network," *Computer*, vol. 30, no. 4, pp. 31–36, Apr. 1997.
- [12] H. A. Rahman *et al.*, "Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports," *Int. J. of Critical Infrastructures*, vol. 5, no. 3, Jan. 2009.
- [13] P. Cholda *et al.*, "Towards risk-aware communications networking," *Rel. Eng. & Sys. Safety*, vol. 109, pp. 160–174, January 2013.
- [14] "Sikkerhet og beredskap mot ekstremvær i telesektoren," [Security and preparedness for extreme weather situations in the telecommunication sector], Working Group Energi Norge and Telenor, [http://www.energinorge.no/getfile.php/FILER/TEMAER/NTech\\_Rep\\_2013](http://www.energinorge.no/getfile.php/FILER/TEMAER/NTech_Rep_2013).
- [15] P. E. Heegaard *et al.*, "Survivability as a generalization of recovery," in *Proc. DRCN*, March 2015.
- [16] "ITU-T, terms and definitions related to quality of service and network performance including dependability. recommendation e.800," ITU-T, Tech. Rep., August 1994.
- [17] "Möbius tool." [Online]. Available: <https://www.mobius.illinois.edu/>
- [18] W. H. Sanders and J. F. Meyer, "Stochastic activity networks: Formal definitions and concepts," in *Lectures on Formal Methods and Performances Analysis*. Springer, 2001, vol. 2090.
- [19] "Avbrotstatistikk 2013," [Outage statistics 2013], NVE, Norwegian Water Resources and Energy Directorate, November 2014.
- [20] G. Kjølle *et al.*, "Incorporating short interruptions and time dependency of interruption costs in continuity of supply regulation," in *CIREC, Prague, Czech Republic*, 2009, pp. 1–4.



---

## Managed Dependability in Interacting Systems

Poul E. Heegaard, Bjarne E. Helvik, Gianfranco Nencioni, and Jonas Wäfler  
In Lance Fiondella, Antonio Puliafito (Eds.), *Principles of Performance and Reliability Modeling and Evaluation*. Springer.

This book chapter is accepted for publication and is going to be published in 2016





# Managed dependability in interacting systems

Poul E Heegaard, Bjarne E Helvik, Gianfranco Nencioni, Jonas Wäfler

**Abstract** A digital ICT infrastructure must be considered as a system of systems in itself, but also in interaction with other critical infrastructures such as water distributions, transportation (e.g. Intelligent Transport Systems), and Smart Power Grid control. These systems are characterised by self-organisation, autonomous subsystems, continuous evolution, scalability and sustainability, providing both economic and social value. Services delivered involve a chain of stakeholders that share the responsibility, providing robust and secure services with stable and good performance.

One crucial challenge for the different operation/control centers of the stakeholders is to manage dependability during normal operation, which may be characterised by many failures of minor consequence. In seeking to optimise the utilisation of the available resources with respect to dependability, new functionality is added with the intention to help assist in obtaining situational awareness, and for some parts enable autonomous operation. This new functionality adds complexity, such that the complexity of the (sub)systems and their operation will increase. As a consequence of adding a complex system to handle complexity, the frequency and severity of the consequences of such events may increase. Furthermore, as a side-effect of this, the preparedness will be reduced for restoration of services after a major event (that might involve several stakeholders), such as common software breakdown, security attacks, or natural disaster.

This chapter addresses the dependability challenges related to the above mentioned system changes. It is important to understand how *adding complexity to handle complexity* will influence the risks, both with respect to the consequences and the probabilities. In order to increase insight, a dependability modelling approach is taken, where the goal is to combine and extend the existing modelling approaches in a novel way. The objective is to quantify different strategies for management of de-

---

Poul E Heegaard, Bjarne E. Helvik, Gianfranco Nencioni, Jonas Wäfler  
Norwegian University of Science and Technology, Department of Telematics, Trondheim, Norway,  
e-mail: {firstname.lastname}@item.ntnu.no

pendability in interacting systems. Two comprehensive system examples are used to illustrate the approach. A Software Defined Networking example addresses the effect of moving control functionality from being distributed and embedded with the primary function, to be separated and (virtually) centralised. To demonstrate and discuss the consequences of adding more functionality both in the distributed entities serving the primary function, and centralised in the control centre, a Smart Grid system example is studied.

## 1 Introduction

The private and public ICT service-provisioning infrastructure has developed over many years into a complex system and its interactions with other critical infrastructure systems such as water distributions, transportation (e.g. Intelligent Transport Systems), and Smart Power Grid control have created diverse digital ecosystems. Digital ecosystems are characterised by self-organisation, autonomous subsystems, continuous evolution, scalability, and sustainability, providing both economic and social value. Services delivered involve a chain of stakeholders that share the responsibility, providing robust and secure services with stable and good performance.

This evolution has been evident for some time. In spite of this, and the crucial role of such systems, not much research is directed toward ensuring the dependability of the services provided by such ecosystem of systems. The objective of this chapter is to address some of the issues that arise when we seek to manage the dependability of systems.

### 1.1 Challenges

One crucial challenge for the different operation and control centres of the different systems is to manage the dependability in normal operation with many failures of minor consequence. In seeking to optimise the utilisation of the available resources with respect to dependability [1], the complexity of the (sub)systems and their operation will increase due to increased interconnectedness and complexity.

Some issues to take into consideration include:

- The public ICT services are the result of the cooperation between a huge number of markets actors. The overall system providing these services are not engineered, and there is no aggregate insight into their design and operation.
- There is no coordinated management to deal with issues involving several autonomous systems, in spite of such issues being a likely cause of extensive problems and outages.
- It is necessary to prepare for restoration of service after a major event such as common software breakdown, security attacks, or natural disasters. This prepa-

ration must include technical and operational as well as organisational and societal aspects.

An additional challenge is the management of dependability over multiple network domains, with uncoordinated operations in each of the different domains. As a potential side-effect of this, the preparedness for restoration of services after a major event (that might involve several stakeholders) such as common software breakdown, security attacks, or a natural disaster will be reduced. In addition, the frequency and consequences of such events may increase. More focus on exercises and use of the improved situational awareness provided by the new operational functionality, will to some extent reduce the negative side effect.

Ensuring the dependability of services based on an interacting relationship between independent stakeholders in the provision is typically agreed upon through Service Level Agreements (SLAs), which give guarantees on the non-functional properties of the services, including dependability aspects such as interval availability. These are important means to ensure the dependability of the services, but are insufficient to prevent and handle dependability problems across providers, as outlined above.

New functionality is added to enhance and improve operation and management of complex digital ecosystems. This is done to rationalise the operation, save money, simplify resource management, and maximise utilisation. It also enables more timely and precise knowledge and information about system state, facilitating timely (proactive) maintenance, and reducing the frequency and consequences of failures. The operational cost is reduced by reduction in manual labour through better and quicker detection and diagnostic mechanisms, and more autonomous self-repair. The objective is to shorten the recovery time and to reduce the failure frequency through better proactive maintenance. It should be kept in mind that this functionality targets the frequent (everyday) failures which are anticipated in the system design and normally of low consequence. However, this increased maintainability is achieved by the introduction of new, and partly centralised functionality, that increases the total complexity and creates an interdependent system [8]. These systems not only have additional failures and failure modes [12, 22], but they may also manifest a more fragile behaviour in critical situations [2, 18].

Figure 1 illustrates a risk curve, where the events with high “probability” have low consequence and the events with low “probability” have high consequence. The introduction of ICT-based support system, to operate an ICT system, or a critical infrastructure such as Smart Grid, is expected to reduce the consequences and probability of daily events. Less human resources are needed for the daily operations. However, due to the introduction of another ICT-based system, the complexity and interdependency in a system will increase, with the potential consequence of increased probability of critical events with extensive and long lasting consequences. Such events affect large parts of the system and a take long time to recover from because of lack of understanding of the complexity (“we have not seen this failure before”), or the lack of maintenance support and coordination between the different subsystems and domains in the digital ecosystem (“who should do what?”). As indicated in the figure, it is not only necessary to increase the focus and manpower

on the events with larger consequences, but also increase the competence of the operation personnel.

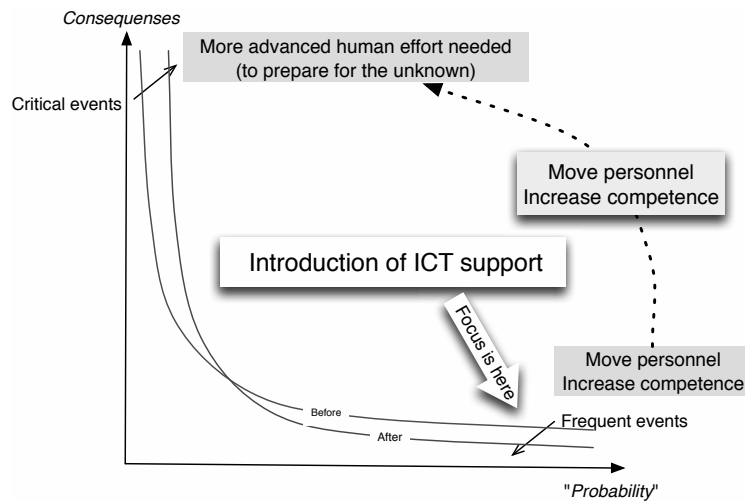


Fig. 1 Introducing ICT support to assist daily operations may increase the overall risk

There is a lack of theoretical foundation to control the societal and per service dependability of ICT infrastructure in the digital ecosystem. No foundation is established for optimisation, consolidated management, and provision of this infrastructure, neither from a public regulatory perspective, nor from the perspective of groups of autonomous (commercially) co-operating providers. A model of an ICT infrastructure must describe the structure and behaviour of the physical and logical information and network infrastructure, and include the services provided. Furthermore, through the modelling phases, it should be described how *resilience engineering* [9] can be applied to manage the robustness and survivability of the ICT infrastructure ecosystem.

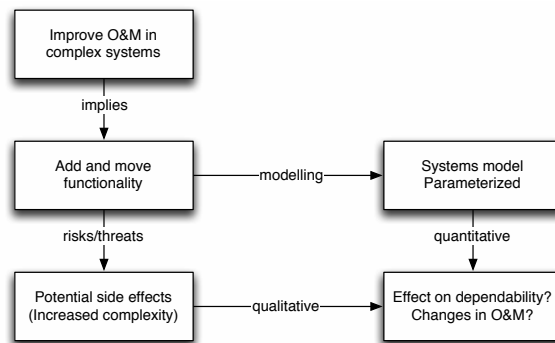
## 1.2 Outline

This chapter describes the above mentioned challenges and outlines potential approaches to gain more insight into the risks. To increase the understanding and assess the risk (both consequences and probabilities), a holistic modelling approach is taken of service in systems of systems. The goal is to quantify different strategies for management of dependability in interacting systems. This should be addressed by different approaches:



- *System modelling*: Modelling of the functional interaction between embedded technical sub-systems in an ecosystem with multiple actors coordinated via business models only.
- *Management strategies*: Management and provisioning of (digital) ecosystems in a cost-efficient way, considering the trade-off between cost and quality.
- *Quantitative assessment*: Resource allocation optimisation (modelling, measurements, simulations) of robustness/dependability and performance in digital ecosystems.

Figure 2 illustrates that to improve the operation and management (O&M) of complex systems (e.g. in the Smart Grids), new control logic and functionality must be added and in some cases also be centralised (e.g. in Software Defined Networking (SDN), and by the introduction of network function virtualisation NFV in next generation communication networks). This needs to be modelled, and the system models parametrised to quantify the effect on the dependability and to identify potential changes and improvements that can be made in O&M. The reason is that the new and/or moved functionality poses new risks and threats to the systems, and may have potential undesired side-effects that need to be qualitatively assessed to again identify potential changes and improvements that can be made during O&M, and to the O&M systems.



**Fig. 2** Understanding the complexity

As a step towards gaining this understanding, Section 2 discusses how the complexity is changing by adding and moving control logic from being embedded and closely integrated with the functionality to be controlled to being separated and to some extents also centralised. Being able to deal with these issues, the ability to build representative, yet understandable and tractable dependability models are crucial. Seeking to build an entirely new theoretical approach does not seem feasible. Our approach is to extend and combine current approaches in novel manners to reach our objective. Hence, to illustrate this and to exemplify the effect of the changes in complexity, Section 2 includes two simple models with numerical exam-

ples. To demonstrate how the complexity might be modelled and assessed, Section 3 gives an example of modelling of the increase complexity in SDN, and Section 4 provides the same for a Smart Grid example. Finally, our concluding remarks are found in Section 5.

## 2 Complex digital ecosystems

As discussed in the previous section, digital ecosystems are complex systems, which are challenging to operate and control. This is due both to their tight integration with other technical systems and the necessity to perform management over multiple system domains where each domain has (partly) uncoordinated operations.

To enhance and improve the operation and maintainability of the complex digital ecosystems, new functionality is *added* and/or *moved and centralised*. As an example, in Software Defined Networking, the functionality of the control logic is separated from the forwarding functionality in the data plane and *moved* from the distributed control plane residing on the components to be controlled to a virtually centralised control plane. Another example is Smart Grid, where the ICT and power grids are tightly integrated and interdependent. New functionality is *added* both in a distributed manner to enable observability and controllability of the components in the power grid, and centralised in the control centres to implement the control and management.

Adding and moving functionality will contribute to changes in the complexity. The goal is to simplify, or assist handling of complexity. However, adding new hardware and software, or moving the existing, will change the interrelations between functional and logical “entities”/“components”. This means that, even though the total complexity is the same or reduced, the system is less well understood and potentially contains new vulnerabilities and poses new management challenges.

Later in this chapter, two comprehensive system examples are introduced to demonstrate the modelling of this change in complexity. In Section 3, a model of Software Defined Networking is given and in Section 4 a Smart Grid example.

### 2.1 Centralising distributed functionality

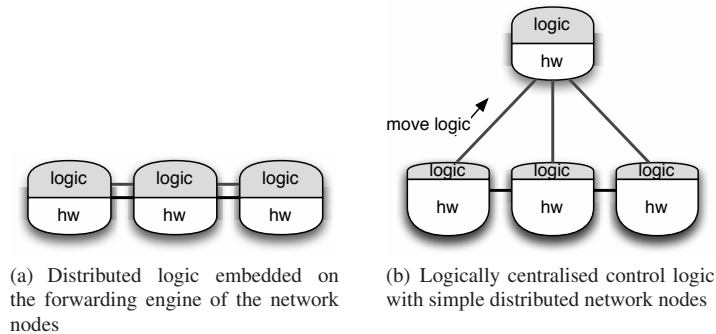
IP networks are comprised of distributed, coordinated, but autonomous network nodes, where the control logic is embedded and closely integrated with the same forwarding functionality that is to be controlled, as illustrated in Figure 3(a).

In emerging networking technology, the trend is to separate the control and forwarding<sup>1</sup> and to move the control logic from the network nodes to a (virtually) centralised controller. The reduction in the distributed (control logic) functionality and

---

<sup>1</sup> This is similar to how it was done in telephony systems (PSTN) with separate data traffic and signalling traffic using Signalling System 7 (SS7) [10] and in B-ISDN [11]

a corresponding increase in the centralised functionality will potentially reduce the complexity in the (partly) autonomous network nodes and increase the complexity of the centralised systems, as illustrated in Figure 3(b).



**Fig. 3** Moving control logic to enhance the resource utilisation and improve QoS

It is reasonable to assume that a simplification in the functionality will reduce the complexity of the network nodes. If the properties of the hardware platform is unchanged the network node will then be less error prone. However, if at the same time commodity hardware is used to reduce the node cost then there is a potential risk of decreasing the hardware availability. Then, it is not obvious whether the node availability will improve or not.

The centralisation of the complex functionality should increase the system availability, due to better global overview and coordination. The control logic has comparable (or the same) functionality to the functionality that is moved from the distributed nodes, but additional functionality is needed to coordinate and mitigate the central controllers. Furthermore, centralisation invites new more advanced functionality, for instance consult the motivation for SDN, [6, 20, 24]. It is therefore not known what effect the central controllers have on the system availability.

A separation of the forwarding and control functionality does not necessarily mean a separation of the hardware platform and its functionality. A common mistake is to forget that the underlying resources, such as the routing and switching hardware, are typically utilised not only by the primary information handled by the system, such as user packets, but also for the signalling of information exchange necessary to control and manage the very same resources. Such an interdependency has a negative effect on the overall system availability [4].

Whether the system availability is improved or not when centralising complex functionality depends on to what extent the reduced complexity of the functionality will have a positive effect and improve resource utilisation (due to the global system state being available, which eases resource coordination) compared to the added complexity in the overhead associated with managing the centralised functionality.

**Example 1: Availability requirement of the controller.** To demonstrate the effect of moving the complexity on availability a very simple example can be considered. Assume that the conventional network in Figure 3(a) is modelled as a serial structure with three network nodes with availability  $A_{No}$ . The serial structure of the network nodes is assumed for simplicity and is not regarded as realistic. The new network is a serial structure consisting of the central controller with availability  $A_C$  and the three networks nodes with availability  $A_{Nn}$ . Since moving the complexity should improve the availability then  $A_{No} < A_{Nn}$ . The availability requirement of the controller is given by

$$A_C > \left(\frac{A_{No}}{A_{Nn}}\right)^3 \quad (1)$$

If  $A_{No} = 0.98$  and  $A_{Nn} = 0.99$ , then  $A_C > 0.97$ .

If we have some inherent redundancy in the distributed system the effect becomes radical. Assuming the elements in the network in Figure 3(a) operate in a ideal load-shared mode where on them can take the entire load. They will then constitute a parallel system and we get  $A_C^* \cdot 1 - (1 - A_{Nn})^3 > 1 - (1 - A_{No})^3$ , where  $A_C^* > 0.999992$ .

Later, in Section 3, a system model of Software Defined Networking is introduced to address in more detail the effect of moving control functionality from being distributed and embedded with the primary function to be separated and (virtually) centralised.

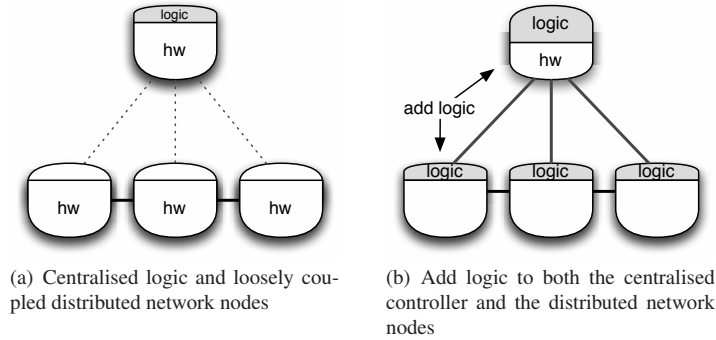
## 2.2 Add distributed and increase centralised functionality

The need for enhanced operation and control in the power grid is an excellent example where new ICT based control logic is added to the distributed power grid components. In power distribution grids, the grid components typically contain little or no automated control logic. This means that manual detection and recovery is required, which must be coordinated by the control centre, as illustrated in Figure 4(a).

Figure 4(b) shows that new functionality must be added to the centralised controller to be able to utilise the new distributed functionality (remote control logic). Centralising functionality to achieve better decisions will provide a single point of failure, performance bottleneck, and expose targeted attacks.

The ICT based control functionality is not only supporting the operations, but needs to be operated in addition to the primary functionality. The technology and functionality will in many cases be new to the organisation and might change the workflows and result in a need for enhanced knowledge and competence in operation.

From a dependability perspective, adding ICT based control seems to be a bad idea since all the negative side-effects pointed out in the previous subsection apply, with functionality added both in the distributed nodes and in the centralised controllers. This produces less positive effects compared to moving and centralising



**Fig. 4** Adding control logic to enhance the maintainability and improve service reliability

functionality. However, the new ICT based control functionality will increase the maintainability through more timely and precise knowledge and information about system state, so timely (proactive) maintenance can be carried out, and hence, the frequency and consequences of the most frequent faults (failures) are reduced. The operational cost is reduced by reduction in manual labour through better and quicker detection mechanisms and more autonomous (self-)repair. The results are reduced recovery times and better proactive maintenance.

It is not guaranteed that the system availability will increase from added (ICT-based) functionality or not. Even though the maintainability is significantly improved, which makes both proactive and reactive maintenance more effective, it is an uncertainty in that the control functionality itself adds complexity that might affect the system availability.

**Example 2: Mean component down time.** Adding more logic to the components is assumed to reduce the components recovery time, but at the same time increase the component failure intensity. The hardware failure intensity is assumed unchanged, but the added logic might also fail.

To compare the two systems we should consider the requirements of mean down time (MDT), mean time to failures (MTTF), and availability. In this example, we say that the new system should have the same availability requirement and will then determine the maximum MDT requirement of the component for a given set of failure intensities for the hardware,  $\lambda_H$ , and software,  $\lambda_S$ .

The availability of the original system is:

$$A_{No} = A_{So} \cdot A_H^3 = \frac{\mu_S}{\lambda_S + \mu_S} \cdot \left( \frac{\mu_H}{\lambda_H + \mu_H} \right)^3 \quad (2)$$

while for the modified system with added functionality it is:

$$A_{No} = A_{Sn} \cdot (A_{HS} \cdot A_H)^3 = \frac{\mu_S}{\mu_S + \lambda_{SS}} \cdot \left( \frac{\mu_S \mu_{SS}}{(\lambda_S + \mu_S)(\lambda_H + \mu_{SH})} \right)^3 \quad (3)$$

To retain the same availability level in the new system, the maximum mean down time  $MDT = 1/\mu_{HS}$  is determined by  $A_{No} < A_{Nn}$ . Let the software failure intensity [in minutes<sup>-1</sup>] for the centralised control logic be  $\lambda_{SS} = 0.5\lambda_S$ , and  $\lambda_H = 1/24$ ,  $\mu_S = 60$ ,  $\lambda_H = 1/168$ ,  $\mu_H = 1$  then  $\mu_{HS} > 1.18529$ , which means that  $MDT < 50.6$  minutes.

In Section 4, a Smart Grid example is introduced to demonstrate and discuss the consequences of adding more functionality, both in the distributed entities serving the primary function and centralised in the control centre.

### 3 Example: Availability in Software Defined Networking

The purpose of this section is to present a case study that highlights how the complexity changes by moving the control logic of a system from distributed to centralised. To illustrate this, we extend and combine current approaches in order to model and assess the availability of a new network paradigm. The results show how the management of complex systems is critical from a dependability perspective. In the following, we introduce some details about Software Defined Networking (SDN) and describe the problem addressed, then we present a two-level hierarchical model for to evaluate the availability of SDN. Finally, we perform a simple sensitivity analysis on a selected set of parameters that will potentially affect the dependability of SDN.

#### 3.1 Software Defined Networking

During the recent years, the SDN has emerged as a new network paradigm, which mainly consists of a programmable network approach where the forwarding plane is decoupled from the control plane [6, 14]. Despite programmable networks having been studied for decades, SDN is experiencing a growing success because it is expected that the ease of changing protocols and provide support for adding new services and applications will foster future network innovation, which is limited and expensive in todays legacy systems.

A simplified sketch of the SDN architecture from IRFT RFC 7426 [6] without the management plane is depicted in Figure 5. The control plane and data plane are separated. Here the control plane is logically centralised in a software-based controller (“network brain”), while the data plane is composed of the network devices (“network arms”) that conduct the packet forwarding.

The control plane has a northbound and a southbound interface. The northbound interface provides an network abstraction to the network applications (e.g. routing protocol, firewall, load balancer, anomaly detection, etc...), while the southbound

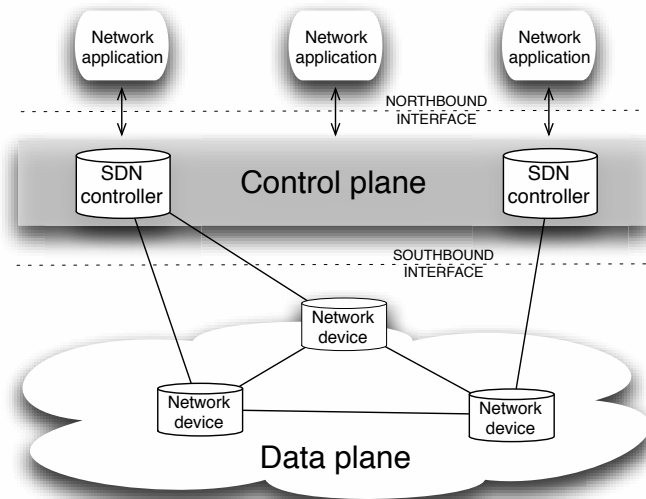


Fig. 5 SDN architecture (exclusive the management plane)

interface (e.g. OpenFlow) standardises the information exchange between control and data planes.

In [20], the following set of potential advantages of SDN were pointed out:

- centralised control;
- simplified algorithms;
- commoditising network hardware;
- eliminating middle-boxes;
- enabling the design and deployment of third-party applications.

However, from a dependability perspective, the SDN poses a set of new vulnerabilities and challenges compared with traditional networking, as discussed in [7]:

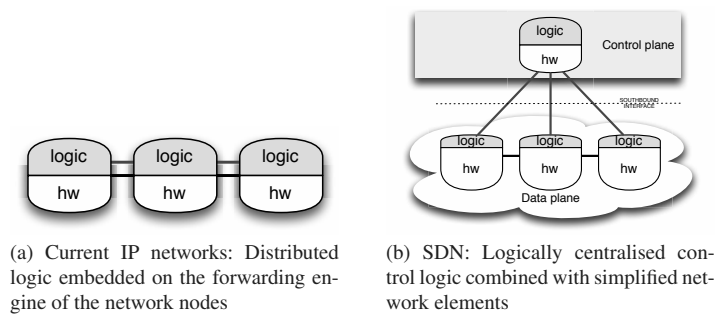
- consistency of network information (user plane state information) and controller decisions;
- consistency between the distributed SDN controllers in the control plane;
- increased failure intensities of (commodity) network elements;
- compatibility and interoperability between general purpose, non-standard network elements
- interdependency between path setup in network elements and monitoring of the data plane in the control plane;
- load sharing (to avoid performance bottleneck) and fault tolerance in the control plane have conflicting requirements;

### 3.2 Problem description

Traditional IP networks consist of a set of interconnected nodes that include both the data and control planes. Each network node is a complex device that has the functionality of both data forwarding and networking control. To increase the availability and performance of such devices, manufacturers have focused on specialised hardware and software over the past few decades.

As discussed in Section 2, SDN has the potential to change the principles of networking and to enhance network flexibility. This implies moving the control logic from the network nodes to a (virtual) centralised controller, and to open up the controllers to a third party via an API (northbound interface), as illustrated in Figure 6. The transition from a *distributed* network with a focus on establishing and maintaining the connectivity between peering points, to a *centralised* network with a focus on QoS and resource utilisation, will potentially lead to much simpler network nodes with less control logic. The centralised control logic, such as the routing decisions, might be simpler and can even be made more advanced, without making it more complex compared to the distributed solution. The controller has the potential to set up data flows based on a richer set of QoS attributes than in traditional IP networks. However, the coordination and handling of the consistency between the SDN controllers, will require new, and complicated logic that will be a critical element to also make SDN a good solution from a dependability perspective.

In the example in this section, we study how the SDN paradigm modifies the overall availability of the network relative to the traditional distributed IP network and analyse which factors dominate in this new scenario.



**Fig. 6** Software Defined Networking is an example where the control logic is moved from distributed to virtually centralised (see Fig. 3)

Although dependability must be regarded as an important issue to make SDN a success, to the best of our knowledge, very limited work on modelling the dependability in SDN availability has been performed. In [17], a model of SDN controllers is developed, while [7] discusses potential dependability challenges with SDN, which is partially illustrated by a small case study with a structural analysis



of SDN enabled network. In this section, we study a comprehensive system model of SDN with respect to dependability.

### 3.3 Modelling

A two-level hierarchical model is introduced to evaluate the dependability of SDN in a global network. In this example, the dependability is measured in terms of steady state availability, in the following referred to as availability. The two-level hierarchical modelling approach consists of

- *upper level*: a structural model of the topology of network elements and controllers
- *lower level*: dynamic models (some) of network elements

The approach seeks to avoid the potential uncontrolled growth in model size, by compromising the need for modelling details and at the same time modelling a (very) large scale network. The detailed modelling is necessary to capture the dependencies that exists between network elements and to described multiple failure modes that might be found in some of the network elements and in the controllers. The structural model disregards this and assumes independence between the components considered, where a component can be either a single network elements with one failure mode or a set of elements that are interdependent and/or experience several failure modes and an advanced recovery strategy. For the former we need to use dynamic models such as a Markov model or Stochastic Petrinet (e.g., Stochastic Reward Network [3]), and for the latter structural models such as reliability block diagram, fault trees, or structure functions based on minimal cut or path sets.

In the following section, we will demonstrate the use of this approach.

#### 3.3.1 Model case

In this example, we analyse the availability of a nation-wide backbone network that consists of 10 nodes across 4 cities, and two dual-homed SDN controllers. See Figure 7 for an illustration of the topology. The nodes are located in the four major cities in Norway, Bergen (BRG), Trondheim (TRD), Stavanger (STV), and Oslo (OSL). Each town has duplicated nodes, except Oslo which has four nodes (OSL1 and OSL2). The duplicated nodes are labelled,  $X_1$  and  $X_2$ , where  $X=OSL1, OSL2, BRG, STV, \text{ and } TRD$ . In addition to the forwarding nodes, there are two dual-homed SDN controllers ( $SC_1$  and  $SC_2$ ), which are connected to TRD and OSL1.

The objective of the study is to compare the availability of SDN with a traditional IP network with the same topology of network elements (SDN forwarding switched and IP routers). We assume that nodes, links, and controllers in the system may fail. The peering traffic in a city is routed through an access and metro network with a connection to both (all four) nodes in the city. The system is working (up), when

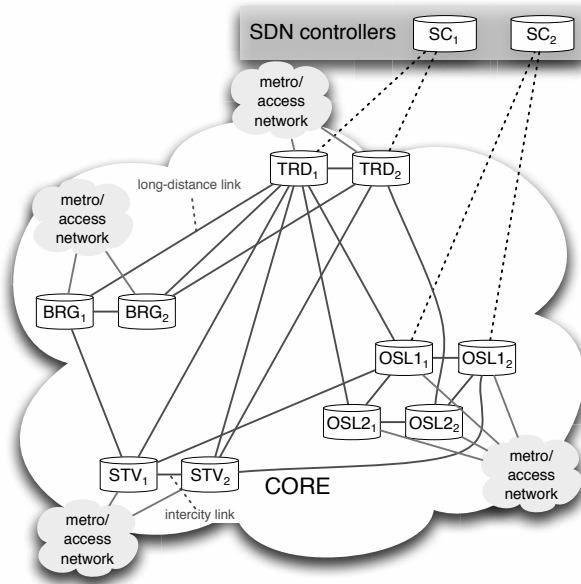


Fig. 7 Case study: nation-wide backbone network

all the access and metro networks are connected. Note that for SDN, at least one controller must be reachable from all nodes along a working path.

### 3.3.2 Structural analysis

The critical parts of the connection between the traffic origins and destinations can be determined using structural analysis based on either *minimal cut sets*,  $S$ , or *minimal path sets*. The sets are defined as follows.

**Definition 1.** *Minimal cut set:* The system is failed if and only if all the subsystems in a minimal cut set are failed, given that all the other subsystems that are not in the set are working.

**Definition 2.** *Minimal path set:* The system is working if and only if all the subsystems in a minimal path set are working, and given that all the subsystems that are not in the set are failed.

We use the *minimum cut sets*,  $S$ , to form the basis for a *structure function*,  $\Phi$  (minimum path sets can also be applied).

**Definition 3.** *Structure function:* Each max-term of the structure function expressed in a minimal product-of-sums form corresponds to a minimal cut set.

The following connections in SDN must be considered:

- *flow triggering*: a path for the trigger message that should be sent from the source node (at least one node of each city) to at least one SDN controller on arrival of a new flow;
- *network state update and route directives*: a path from the SDN controller to each node;
- *forwarding*: forwarding path from/to each city (6 combinations).

The structural analysis for all the possible connections in the SDN example, shows that the cardinality of the set of minimal cut set  $S$  is  $\|S\| = 2916$ . The cardinality  $c_j = \|s_j\|$  of each of the minimal cut sets,  $j = 1, \dots, 2916$  is given in Table 1. Each column contains the number of sets that is  $C_k = \|\{s_j \in S | c_j = k\}\|$ ,  $k = 1, \dots, 13$ . The table compares the minimal cut sets of SDN with a conventional IP network where the control plane is embedded in the nodes, and hence, no controllers are needed.

**Table 1** Distribution of cardinality of the minimum cut sets for the IP network and SDN

	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$	$C_6$	$C_7$	$C_8$	$C_9$	$C_{10}$	$C_{11}$	$C_{12}$	$C_{13}$	sum
IP network	0	3	8	91	304	360	356	189	70	13				1394
SDN	0	4	15	107	340	520	780	584	302	170	59	31	4	2916

The number of minimal cut sets with cardinality one is equal to zero because traffic sources are at least dual-homed and there are two dual-homed control sites.

The number of minimal cut sets  $C_2$  increases from 3 to 4 due to the control nodes. Note also that the number of minimal cut sets  $C_3$  almost doubles. This indicates that in this example, a significant increase in vulnerability is observed for the SDN case that is not explained solely by the introduction of a control node, but the fact that a controller must be reachable from every node across the backbone in order for the network to work.

### 3.3.3 Markov model of networks elements

In order to evaluate the availability of each network element, we develop Markov models of each of the links, traditional routers/switches, SDN routers/switches, and the SDN controllers.

#### *Links*

The network model of a link is assumed to be dominated by hardware failures. Therefore, a simple two-state Markov model is used. The links are either up or down due to hardware failure. We use the same model for both traditional networks and

SDN. Given failure rate  $\lambda_L$  and repair rate  $\mu_L$ , the availability of a link is  $A_L = \frac{\mu_L}{\lambda_L + \mu_L}$ . This model is assumed for each of the components in the structural model.

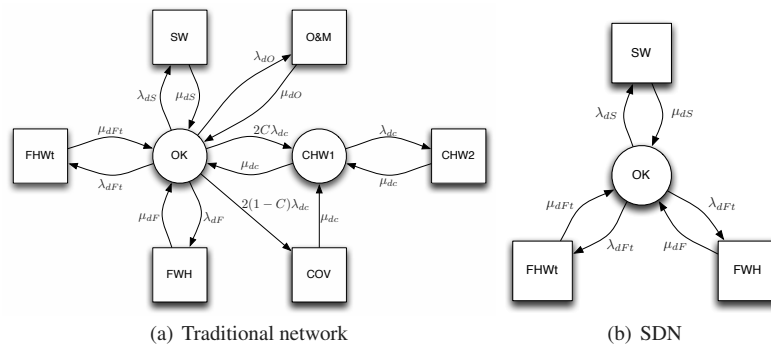
### Routers

The model of a traditional router/switch is depicted in Figure 8(a), where the states are defined in Table 2.

**Table 2** State variables for traditional IP router

state	up/down	description
<i>OK</i>	up	System is fault free
<i>OM</i>	down	Operation and Maintenance state
<i>CHW1</i>	up	Hardware failure of one controller
<i>CHW2</i>	down	Hardware failure both controllers
<i>COV</i>	down	Coverage state, unsuccessful activation of the stand-by hardware after a failure; manual recovery
<i>FHW</i>	down	Permanent hardware failure in forwarding plane
<i>FHWt</i>	down	Transient hardware failure in forwarding plane
<i>SW</i>	down	Software failure

Multiple failures are not included in the model since they are rare and will have an impact significantly smaller than the expected accuracy of the approach.



**Fig. 8** Markov model of a router/switch

### SDN forwarding nodes

Figure 8(b) shows the model of the forwarding node, i.e., router or switch in an SDN, which corresponds to the traditional IP router. It is significantly simpler. The states related to the control hardware and O&M failures are not contained in this model, since all the control logic is located in the controller. The software is still present but its failure rate will be very low since the functionality is much simpler.

### SDN controller

The model of the SDN controller is composed of two sets of states. One set captures the software and hardware failures. The second set captures the O&M failures in combination with the hardware states of the system. We have assumed that the SDN controller is a cluster of  $M$  processors and the system is working, i.e., possesses sufficient capacity if  $K$  out of the  $M$  processors are active, which means that both software and hardware are working. To represent this scenario, each state is labelled by four numbers  $\{n, i, j, k\}$ , where  $n$  is the number of active processors,  $i$  the number of processors down due to hardware failures,  $j$  the number of processors down due to software failures, and  $k$  the state of the O&M functionality ( $k = 1$  if O&M mistake,  $k = 0$ , if not). Figure 9 shows the *outgoing* transitions from a generic state  $\{n, i, j, k\}$ . The main characteristics of the model are:

- single repairman for a hardware failure;
- load dependency of software failure when the system is working,  $\lambda_S(n) = \lambda_S/n$ , where the meaning of  $\lambda_S$  is explained in more detail in Section 3.4;
- load independence of software failure when the system has failed,  $\lambda_S(n) = \lambda_S$ ;
- when the entire system fails, only processors failed due to hardware failures will be down until the system recovers.

### 3.3.4 Using inclusion-exclusion principle to evaluate the system availability

The inclusion-exclusion principle is a technique to obtain the elements in the union of finite sets. Using the inclusion-exclusion principle on the structure function, we can write the system availability as the probability of the union of all minimal paths:

$$A_S = P\left(\bigcup_{i=1}^n Q_i\right) = \sum_{k=1}^n (-1)^{k-1} \sum_{\substack{\emptyset \neq I \subseteq [n] \\ |I|=k}} P\left(\bigcap_{i \in I} Q_i\right), \quad (4)$$

where  $\{Q_1, Q_2, \dots, Q_n\}$  is the set of all minimal paths, and  $P(Q_i)$  is the probability of set  $Q_i$ .

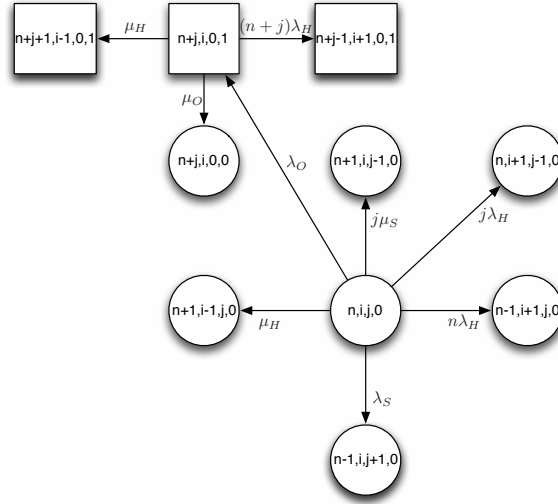


Fig. 9 Generic states of the model of SDN controller

To compute the probability of the intersection of minimal paths, we need to know the availability of each network element. To this end, we can calculate the element availability by using the proposed Markov models.

### 3.4 Numerical evaluation

To evaluate the availability of traditional networks, we consider the typical parameters in Table 3, which are inspired by and taken from several studies [5, 15, 23].

All SDN parameters are expressed relative to the parameters for the traditional network (Table 3). The parameters for the SDN switch you find in Table 4 and for the SDN controller in Table 5. The parameters  $\alpha_H$ ,  $\alpha_S$ , and  $\alpha_O$  are proportionality factors that are studied in this example.

Using these parameters in the models described in this section, we can compare the (un)availability of traditional IP and SDN networks. Failures with the same cause, have the same intensities in both models. However, we assume that the software on an SDN switch/router will be much less complicated than on a traditional IP router, and we have set the failure rate to zero, for the sake of simplicity. In an SDN controller, all failure rates are  $N$ -times larger than in the traditional network, where  $N$  is the number of network nodes. This is because we assume that the centralised system needs roughly the same processing capacity and amount of hardware. Therefore, the failure intensity is assumed to be proportional to  $N$ , and of the

**Table 3** Model parameters for the IP network

intensity	[time]	description
$1/\lambda_L = 4$	[months]	expected time to next link failure
$1/\mu_L = 15$	[minutes]	expected time to link repair
$1/\lambda_{dF} = 6$	[months]	expected time to next permanent forwarding hardware failure
$1/\mu_{dF} = 12$	[hours]	expected time to repair permanent forwarding hardware
$1/\lambda_{dF_t} = 1$	[week]	expected time to next transient forwarding hardware failure
$1/\mu_{dF_t} = 3$	[minutes]	expected time to repair transient forwarding hardware
$1/\lambda_{dC} = 6$	[months]	expected time to next control hardware failure
$1/\mu_{dC} = 12$	[hours]	expected time to repair control hardware
$1/\lambda_{dS} = 1$	[week]	expected time to next software failure
$1/\mu_{dS} = 3$	[minutes]	expected time to software repair
$1/\lambda_{dO} = 1$	[month]	expected time to next O&M failure
$1/\mu_{dO} = 3$	[hours]	expected time to O&M repair
$C = 0.97$		coverage factor

**Table 4** Model parameters for SDN switch/router

intensity	description
$\lambda_F = \lambda_{dF}$	intensity of permanent hardware failures
$\mu_F = \mu_{dF}$	repair intensity of permanent hardware failures
$\lambda_{F_t} = \lambda_{dF_t}$	intensity of transient hardware failures
$\mu_{F_t} = \mu_{dF_t}$	restoration intensity after transient hardware failures
$\lambda_{sS} = 0$	intensity of software failure

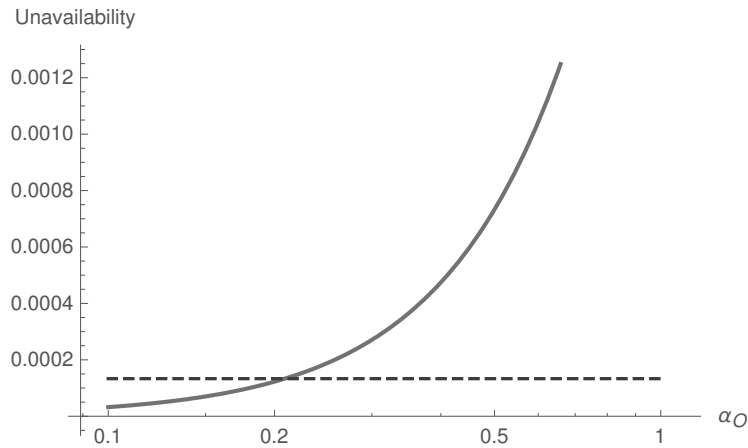
**Table 5** Model parameters for SDN controller

intensity	description
$\lambda_H = \alpha_H \lambda_{dC} N/K$	intensity of hardware failures
$\mu_H = \mu_{dC}$	hardware repair intensity
$\lambda_S = \alpha_S \lambda_{dS} N$	intensity of software failures
$\mu_S = \mu_{dS}$	restoration intensity after software failure
$\lambda_O = \alpha_O \lambda_{dO} N$	intensity of O&M failures
$\mu_O = \mu_{dO}$	rectification intensity after O&M failures

same order of magnitude as the total failure intensity of the traditional distributed IP router system.

The results of a numerical example are given in the plot in Figure 10. The overall unavailability, i.e., the probability that not all cities in Section 3.2 are connected (for SDN this requires also a connection to a controller) is given for different values of  $\alpha_O$ . The figure shows that the unavailability increases with about one order of magnitude when  $\alpha_O$  changes in the range from 0.1 to 1. The sensitivity of  $\alpha_H$  and  $\alpha_S$  are far less significant. This indicates that O&M failures are dominant and most critical to the dependability of SDN.

As a preliminary conclusion from this study, it seems as the use of commodity hardware and centralised control has a moderate effect on the availability of the overall network. However, the O&M failures and software/logical failures that



**Fig. 10** Unavailability of SDN (solid line) and of traditional network (dashed line) by varying  $\alpha_O$  ( $\alpha_H = 1$   $\alpha_S = 1$ )

causes a control cluster to fail are very important in order to improve the dependability when changing from the traditional distributed IP network to SDN.

#### 4 Example: Restoration in Smart Grid

The purpose of this example is to show how the automation of process steps changes the dependability of a system. The system under consideration is a power grid and we focus on the restoration process after a physical failure.

A power grid is a critical infrastructure and its reliability is critical to the smooth operation of a resilient society. Power grids are due to undergo modernisation in the coming years. This next generation power grid is commonly called the smart grid. One of the biggest differences compared to the current grid is additional monitoring information about the current state of the grid and new control abilities throughout the grid. These improvements allow the introduction of more automated processes with the goal of increasing the overall dependability of the system.

This is the starting point of our example. We model the restoration process with and without automation and conduct a dependability analysis. Our results show that the introduction of automation yields benefits like a reduction of down time, but it also extends the system into a compound and more complex system. This system has new failure modes as the automation may malfunction and thus, without taking the appropriate measures, may partially negate benefits.

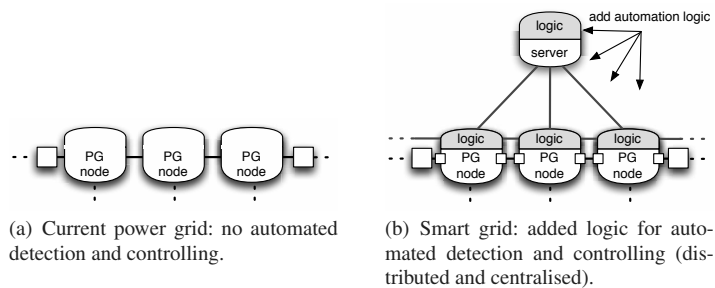


#### 4.1 Problem Description

The power grid (PG) has traditionally contained only a few monitoring and controlling devices distributed throughout the grid. Mostly they are deployed in the higher voltage levels. In the lower voltage levels monitoring and controlling devices are, depending on the country, virtually absent. In case of a failure a distributed and autonomously working protection system automatically disconnects a whole protection zone by opening a circuit breaker, causing a power outage to all customers inside this protection zone.

The future power grid, the so called smart grid, will possess monitoring and control systems widely deployed throughout the power grid. These devices detect failures automatically and send failure diagnostics to a central control, operation, and management system. The central system then attempts to isolate the failure by opening other circuit breakers closer to the failure and connecting the rest of the protection zone again to the grid. It is assumed that the power grid at this voltage level has an open ring topology that allows reconnection to the non-isolated parts after a single failure. Figure 11 shows a protection zone in the current PG and in the smart grid, consisting of three PG nodes and two protection devices represented by large squares. The small squares represent new circuit breakers controlled by the centralised control system.

In the following, we study how the introduction of detection and isolation automation changes the characteristics of the restoration process. More precisely, we study the downtime and the energy not supplied (*ENS*), which is the accumulated energy that could not be delivered due to outages, i.e., down time weighted with the load during the outages. Both the lines and the PG nodes can fail, but only larger outages that require a repair crew to go on site are considered.



**Fig. 11** Schematic view of a protection zone in the current power grid and smart grid.

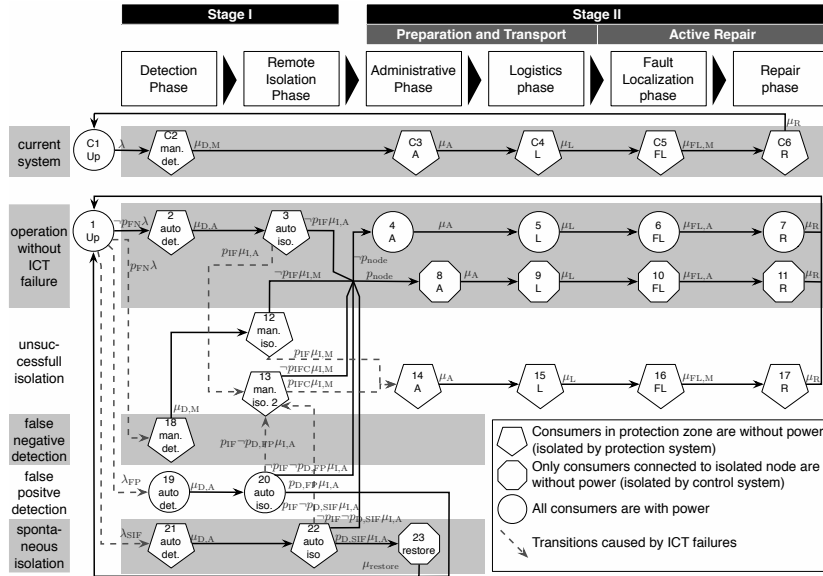


Fig. 12 Phases during the restoration process. For readability reasons, the transitions into state 4 and 8 are displayed in a compact form, it is read as follows; States 3, 12, 13, 20 and 22 each have a transition to 4 and 8, The first is multiplied with  $\neg p_{node}$ , i.e.  $(1 - p_{node})$ , the latter with  $p_{node}$

## 4.2 Modelling

The restoration process of a power grid failure consists of two stages containing a total of six phases, as shown in Figure 12. The phases are:

**Detection** Time period between a failure and its detection in the monitoring system. It is assumed that the protection system disconnects the protection zone containing the failure immediately after the incident. In reality, there is a short delay of several milliseconds. The disconnection leads to a black out in the whole protection zone.

**Remote Isolation** The failed element is isolated more precisely, either automatically by the central system or manually by a controller at the control centre. The rest of the protection zone is powered up again.

**Administrative** Failure diagnostics from the monitoring devices are evaluated, the recovery is planned, and a repair crew is assigned.

**Logistic** Repair crew is equipped with the necessary material and moves to the incident location.

**Fault Localization** Precise localisation of the failure, both geographically and in the system.

**Repair** Actual repair, all isolated network elements are restored to normal operation.

The difference between the current power grid and the smart grid lies mainly in *Stage I*. In the current power grid, detection occurs manually, i.e., the failure is detected by a controller or through a call by a consumer. There are no remote isolation capabilities, so this phase is skipped. Throughout the entire restoration phase, the whole protection zone is without power in the model in Figure 12. This is denoted by pentagonal states.

In the smart grid, the distributed devices detect the failure automatically and send an alarm together with fault diagnostics to the central system. Now, the failure is isolated automatically and remotely from the central system and *Stage II* begins. If a PG node is affected by the failure, and now isolated, then the system proceeds to state 8. If only a line is isolated then it proceeds to state 4. In the first case, there are still consumers without power. In the latter case, the power supply has been reinstated to all consumers. This difference is indicated in the model by the different shapes of the states. In both cases, the number of consumers affected is smaller than in the current system. An additional difference is the sojourn time of the fault localisation phase. It is shorter for the smart grid, as the detection devices provide fault diagnostics that accelerate this phase.

So far, we have described the process during operation without any failures in the new system. In the following, we consider failures in the information and communication technology (ICT) subsystem used for the automation. It is assumed that all the other systems, e.g., the protection system, work perfectly. The following failures in the detection system are considered:

- **false positive detection failure:** there is no failure, but the detection system reports one.
- **false negative detection failure:** there is a failure but the detection system does not notice it.

A *false positive detection failure* is modelled with a new transition out of state 1 with an additional failure intensity leading to state 19. The failure is detected by the system as before. If the system discovers the false positive failure the restoration process is interrupted and the system goes back to state 1, otherwise it continues.

A *false negative detection failure* is modelled by splitting the transition from state 1 to 2 into two, pointing one to state 18 and weighting the rate by the false negative probability  $p_{FN}$ . The new state 18 indicates a manual detection because of the non-detection in the system. The isolation is then done manually by an operator. If the isolation is successful it proceeds as before either in state 4 or 8 depending on whether a line or a node is affected. If the isolation is not successful the entire protection zone remains without power for *Stage II* of the restoration process.

In the isolation system, the following failures are considered:

- **isolation failure:** there is a failure, but isolation is unsuccessful because of problems with communication or systems. The whole protection zone remains unpowered.

- **spontaneous isolation failure:** there is no failure, but a network element is falsely isolated by the system.

An *isolation failure* is modelled in the system by splitting the transitions from the isolation states 3, 12, 13, 20, and 22 into two, and weighting the rate by the probability of an isolation failure  $p_{IF}$ , except for the transitions from 13, which uses a higher probability  $p_{IFC}$ , because the system already suffered one ICT failure and is in a critical state.

A *spontaneous isolation failure* is modelled with a new transition out of state 1 with an additional failure intensity leading to state 21. The failure is detected by the system as before. If the system discovers that the failure originates from the isolation system and not the power grid it restores the system (state 23) and goes back to the up state, otherwise it continues.

### 4.3 Numerical Example

All event times in the system are assumed to be exponentially distributed with the following expected values. The event times are based on data for longer outages from the Norwegian regulator [21].

**Table 6** Model parameters for the IP network

intensity	[time]	description
$1/\lambda = 4$	[months]	expected time to next PG failure inside this protection zone
$1/\lambda_{FP} = 6$	[months]	expected time to next false positive detection failure
$1/\lambda_{SIF} = 12$	[months]	expected time to next spontaneous isolation failure
$1/\mu_{D,M} = 20$	[minutes]	expected manual detection time
$1/\mu_{D,A} = 1$	[minutes]	expected automatic detection time
$1/\mu_{I,M} = 5$	[minutes]	expected manual isolation time
$1/\mu_{I,A} = 1$	[minutes]	expected automatic isolation time
$1/\mu_A = 5$	[minutes]	expected time in administrative state
$1/\mu_L = 15$	[minutes]	expected time in logistics state
$1/\mu_{FL,M} = 20$	[minutes]	expected manual fault localisation time, i.e. without fault diagnostics from the detection devices.
$1/\mu_{FL,A} = 10$	[minutes]	expected automatic fault localisation time
$1/\mu_R = 10$	[minutes]	expected repair time
$1/\mu_{restore} = 10$	[minutes]	expected restoration time for discovered spontaneous isolation failure
$p_{node} = 0.1$		probability of failure affecting a node
$p_{FN} = 0.01$		probability of false negative detection failure
$p_{D,FP} = 0.2$		probability of discovering a false positive in isolation phase
$p_{D,SIF} = 0.2$		probability of discovering a spontaneous isolation failure in isolation phase
$p_{IF} = 0.1$		probability of unsuccessful isolation
$p_{IFC} = 0.5$		probability of unsuccessful isolation (ICT failure)

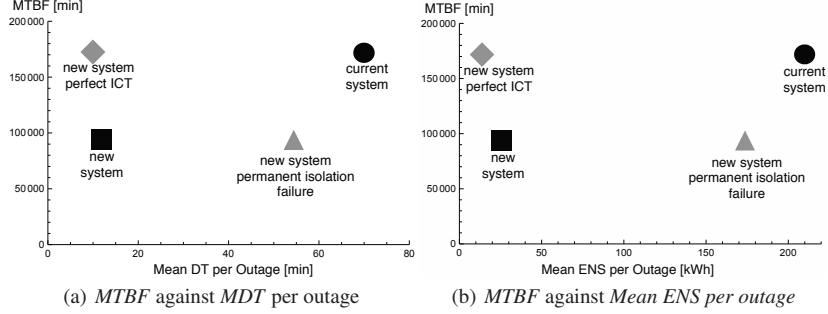


Fig. 13 Mean values per outage

First, we compute *MDT* and the mean time between failure (*MTBF*) for the model in Figure 12. All states in which there is a power outage are considered as down states, i.e. all states but the round states. *MTBF* is computed with

$$MTBF = 1 / \left( \sum_{i \in \Omega_{Up}} \sum_{j \in \Omega_{Down}} \lambda_{ij} p_i \right)$$

where  $p_i$  is the steady state probability of being in state  $i$ ,  $\lambda_{ij}$  is the transition rate from state  $i$  to  $j$ , and  $\Omega_{Up}$  and  $\Omega_{Down}$  are the sets of up and down states respectively. *MDT* is computed by  $MDT = U \cdot MTBF$ , where the unavailability  $U$  is computed with  $U = \sum_{i \in \Omega_{Down}} p_i$ .

The results are presented in Figure 13(a). Four scenarios are computed:

1. current system, which is today's power grid system
2. new system,
3. new system with perfect ICT, i.e.  $p_{FN} = 0$ ,  $p_{IF} = 0$ ,  $\lambda_{FP} = 0$ ,  $\lambda_{SIF} = 0$ , and
4. new system with a permanent isolation failure, i.e.  $p_{IF} = 1$ .

The *MDT* of the new system is smaller than the current system, due to the reduced event times. However, when considering the new system with imperfect ICT, the *MTBF* is reduced as well. Hence, the reduction in *MDT* comes at the expense of more frequent failures. In case of a permanent isolation failure, the *MDT* increases significantly but is still shorter than the current system, as the time in the detection phase is reduced.

*MDT* gives a one-sided picture of the situation, as the down states have different consequences for the system. The consequences are marked in the model with three different shapes. To incorporate this information, we use the concept of Energy Not Supplied (*ENS*). *ENS* is used in outage reports in power engineering and plays a central role in the Norwegian regulation framework [13]. As the name suggests, it indicates the amount of energy that could not be supplied due to an outage. For our example, we assume that each PG node has a constant energy consumption of 1 kWh per minute. In the pentagonal states, three nodes are down. Therefore, the

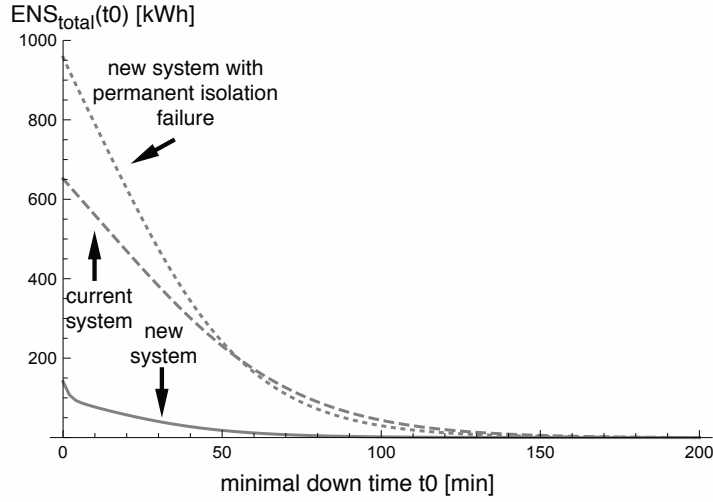


Fig. 14  $ENS_{total}(t_0)$  of failures with downtimes  $> t_0$

$ENS$  is 3 kWh per minute. The octagonal states have an  $ENS$  of 1 kWh per minute and the round states 0 kWh per minute.

We use a Markov reward model to obtain the instantaneous  $ENS$   $e(t)$ , i.e., the energy that cannot be delivered at time instance  $t$ . First, state 1 is defined to be absorbing. When the system is in steady state, a down period starts in state  $j \in \Omega_{Down}$  with probability  $p_j(0) = MTBF \cdot \sum_{i \in \Omega_{Up}, j \in \Omega_{Down}} \lambda_{ij} p_i$ . Now the instantaneous  $ENS$  is computed with  $e(t) = \sum_{i \in \Omega_{Down}} p_i(t) \cdot e_i$ , where  $p_i(t)$  and  $e_i$  are the instantaneous state probability and the energy consumption per minute of state  $i$  respectively.

Integrating  $e(t)$  over time yields *Mean ENS per outage*  $= \int_0^\infty e(t) dt$ , which is plotted in Figure 13(b). The  $MTBF$  is the same as in Figure 13(a). Compared to MDT, the improvement achieved by automation is even larger in this metric because  $ENS$  weighs the downtime according to the consequences. However, this is not true for the case with a permanent isolation failure because the down states are all pentagonal like in the current system.

Finally, we extend *downtime-frequency curves* [19] to characterise how the total  $ENS$  per year of all failures in this protection zone depends on the down time. Let us denote the total  $ENS$  per year with  $ENS_{total}$ . Counting only the  $ENS$  of those outages that are longer than time  $t_0$ , it becomes time dependent and is computed by:

$$ENS_{total}(t_0) = \frac{d(t_0)}{MTBF} \left( \int_{t_0}^\infty \frac{e(t)}{d(t_0)} dt + e^*(t_0) \right)$$

where  $(MTBF)^{-1}$  is the number of failures per year,  $d(t)$  the probability that the system is down at time  $t$ , computed by  $d(t) = \sum_{j \in \Omega_{Down}} p_j(t)$ , and  $e^*(t_0)$  is the

energy not supplied up to time  $t_0$  given that the system has not yet been restored. In order to compute  $e^*(t_0)$ , the Markov model is modified so there is no transition out of the subspace formed by  $\Omega_{\text{Down}}$  because no complete restoration takes place before  $t_0$  by definition. The transition rates are defined as

$$\lambda_{ij}^* = \begin{cases} \lambda_{ij} & \text{if } i, j \in \Omega_{\text{Down}} \\ 0 & \text{otherwise} \end{cases}$$

The initial state vector of the system is  $\mathbf{p}^*(0) = \mathbf{p}(0)$ , as before. Thus,  $\mathbf{p}^*(t)$  and  $e^*(t)$  are computed in the same way as explained above.

The results for  $\text{ENS}_{\text{total}}(t_0)$  are shown in Figure 14. In the current system, the relation between downtimes and  $\text{ENS}_{\text{total}}$  is approximately linear during the first 50 minutes. In the new system, however, there is a drop in the beginning, indicating that short down times contribute disproportionately to  $\text{ENS}_{\text{total}}$ . The drop corresponds to *Stage I* of the model. After that, there are either no consumers without power or the system is in the restoration process with the octagonal or pentagonal states and behaves similarly to the current system but at a reduced level. In the case of a permanent isolation failure,  $\text{ENS}_{\text{total}}(t_0)$  is larger than in the current system for  $t_0 < 55$  minutes, mainly because of the shorter *MTBF*. For larger  $t_0$ , this is compensated for by the effect of shorter *MDT* due to automatic detection. The results show that the automation possesses significant potential to reduce  $\text{ENS}_{\text{total}}$ . However, in case of longer failures, this may become a disadvantage.

#### 4.4 Observations from the example

The automation of the detection and isolation phase is introduced with the goal of reducing *MDT* and *mean ENS per failure*. However, as the new supporting ICT systems may fail as well, the failure characteristics of the system are changed. First, the *MTBF* decreases significantly, i.e. the number of failures per year increases. Second, outages are on average shorter, and short outages become an important factor when the total *ENS* per year is considered. Third, in case of a longer permanent failure in the ICT system, the consequences increase temporarily and, thereby, adversely affect of the benefit of automation.

The introduction of automation should, therefore, be accompanied by two crucial steps. First, additional training is necessary for the staff covering the new failure characteristics and failures, including the scenario of a malfunctioning ICT system [16]. Second, it is necessary to acquire the skills to maintain and quickly restore the new ICT system to assure a high dependability and thus achieve the positive effects for which the automation was originally introduced.

## 5 Concluding remarks

The focus of this chapter has been the increasing complexity in digital ecosystems, which are system-of-systems of ICT infrastructures or interact with other critical infrastructures such as water distribution, transportation (e.g. Intelligent Transport Systems), and Smart Power Grid control. There is a lack of theoretical foundation to control the societal and per service dependability of ICT infrastructure in the digital ecosystem. No foundation has been established for optimisation, consolidated management, and provision of this infrastructure, neither from a public regulatory perspective, nor from the perspective of groups of autonomous (commercially) co-operating providers.

More ICT based operation support and control functions are included to manage digital ecosystems, with the objective to reduce the frequency and consequences of daily events. However, it is important to be aware of the potential side-effects that might increase the frequency and consequences of critical and catastrophic failure events. The reason is that the added support enables interaction and integration of even more complex and heterogeneous systems, changes workflows in organisations, and ICT based support systems may fail.

To enhance and improve the operation and maintainability of complex digital ecosystems, new functionality is *added* and/or *moved and centralised*. Two examples are considered in this chapter: (i) Software Defined Networking, which separates the control logic from the forwarding functionality and *moves* the logic from the distributed network elements to a virtual centralised controller, (ii) Smart Grid integrates ICT and power grids which make them more interdependent. Here, new functionality is *added* both in a distributed manner to enable observability and controllability of the components in the power grid and centralised in the control centres to implement the control.

How the changes in complexity affect the overall system dependability is less understood, contains potential vulnerabilities, and poses new managements challenges. This chapter emphasises the importance of being able to model ICT infrastructures. A model must describe both the structure and behaviour of the physical and logical information and network infrastructure, including the services provided. Furthermore, through the modelling phases, it should be explained how *resilience engineering* can be applied to manage the robustness and survivability of the ICT infrastructure. This is the research focus of the research lab on *Quantitative modelling of dependability and performance*, NTNU QUAM Lab ([www.item.ntnu.no/research/quam/start](http://www.item.ntnu.no/research/quam/start)).

**Acknowledgements** This work is partly funded by Telenor-NTNU collaboration project *Quality of Experience and Robustness in Telecommunications Networks*, NTNU project *The next generation control centres for Smart Grids* (<https://www.ntnu.edu/ime/smartgrids>), COST Action ACROSS (IC1304), and the research lab on *Quantitative modelling of dependability and performance*, NTNU QUAM Lab ([www.item.ntnu.no/research/quam/start](http://www.item.ntnu.no/research/quam/start)).



## References

1. Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C.: Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* **1**, 11–33 (2004)
2. Buldyrev, S.V., Parshani, R., Paul, G., Stanley, H.E., Havlin, S.: Catastrophic cascade of failures in interdependent networks. *Nature* **464**(7291), 1025–1028 (2010)
3. Ciardo, G., Trivedi, K.S.: A decomposition approach for stochastic reward net models. *Perf. Eval* **18**, 37–59 (1993)
4. Cristian, F., Dancy, B., Dehn, J.: Fault-tolerance in the advanced automation system. In: *Fault-Tolerant Computing, 1990. FTCS-20. Digest of Papers., 20th International Symposium*, pp. 6–17 (1990)
5. Gonzalez, A.J., Helvik, B.E.: Characterization of router and link failure processes in UNINETT's IP backbone network. *International Journal of Space-Based and Situated Computing* (2012)
6. Haleplidis, E., Pentikousis, K., Denazis, S., Salim, J.H., Meyer, D., Koufopavlou, O.: Software-defined networking (SDN): Layers and architecture terminology. Request for Comments RFC 7426, Internet Research Task Force (IRTF) (2015)
7. Heegaard, P.E., Mendiratta, V.B., Helvik, B.E.: Achieving dependability in software-defined networking - a perspective. In: *7th International Workshop on Reliable Networks Design and Modeling (RNDM)*. Munich, Germany (2015)
8. Heller, M.: Interdependencies in civil infrastructure systems. *The Bridge* **31**(4) (2001)
9. Hollnagel, E., Woods, D.D., Leveson, N.: *Resilience engineering: Concepts and precepts*. Ashgate (2006)
10. ITU-T: Recommendation Q.700: Introduction to Signaling System No. 7 (1994)
11. ITU-T: Recommendation I.371: Traffic control and congestion control in B-ISDN (1996)
12. Kirschen, D., Bouffard, F.: Keeping the lights on and the information flowing. *IEEE Power and Energy Magazine* **7**(1), 50–60 (2009). DOI 10.1109/MPE.2008.930656
13. Kjølle, G., Samdal, K., Brekke, K.: Incorporating short interruptions and time dependency of interruption costs in continuity of supply regulation. In: *CIREC, Prague, Czech Republic*, pp. 1–4 (2009)
14. Kreutz, D., Ramos, F.M.V., Verissimo, P.J.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: A comprehensive survey. *Proceedings of the IEEE* **103**(1), 14–76 (2015)
15. Kuusela, P., Norros, I.: On/off process modeling of ip network failures. In: *Dependable Systems and Networks (DSN), 2010 IEEE/IFIP International Conference on*, pp. 585–594 (2010). DOI 10.1109/DSN.2010.5544427
16. Line, M.B.: Understanding information security incident management practices: A case study in the electric power industry. Ph.D. thesis, Norwegian University of Science and Technology (NTNU) (2015)
17. Longo, F., Distefano, S., Bruneo, D., Scarpa, M.: Dependability modeling of software defined networking. *Computer Networks* **83**, 280 – 296 (2015)
18. Morris, R.G., Barthelemy, M.: Interdependent networks: the fragility of control. *Scientific Reports* **3** (2013). DOI 10.1038/srep02764
19. Norros, I., Pulkkinen, U., Kilpi, J.: Downtime-frequency curves for availability characterization. In: *IEEE/IFIP Dependable Systems and Networks (DSN)*, pp. 398 – 399 (2007)
20. Nunes, B., Mendonca, M., Nguyen, X.N., Obraczka, K., Turletti, T.: A survey of software-defined networking: Past, present, and future of programmable networks. *Communications Surveys Tutorials, IEEE* **16**(3), 1617–1634 (2014). DOI 10.1109/SURV.2014.012214.00180
21. NVE, Norwegian Water Resources and Energy Directorate: Avbrottsstatistikk 2013. [Outage statistics 2013] (2014)
22. Rinaldi, S., Peerenboom, J., Kelly, T.: Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems* **21**(6), 11–25 (2001). DOI 10.1109/37.969131

23. Verbrugge, S., Colle, D., Demeester, P., Huelsemann, R., Jaeger, M.: General availability model for multilayer transport networks. In: Proceedings.5th International Workshop on Design of Reliable Communication Networks, 2005. (DRCN 2005), pp. 85 – 92. IEEE (2005)
24. Xia, W., Wen, Y., Foh, C.H., Niyato, D., Xie, H.: A survey on software-defined networking. Communications Surveys Tutorials, IEEE **17**(1), 27–51 (2015). DOI 10.1109/COMST.2014.2330903

---

# APPENDIX



---

## Details on Downtime-Frequency Curve and ENS Extension

This appendix gives more information about the formulas and calculations of the *downtime frequency curves* and its extension used in *Paper E*. First, I explain the formula for the downtime frequency curve, then I explain how it can be adjusted to include the energy not supplied.

### A.1 Downtime Frequency Curve

We assume a stationary system with finite downtimes. The downtime distribution is defined as

$$d(t) = P(\text{DT} \geq t) \quad (\text{A.1})$$

i.e. it gives the probability that the downtime (DT) is longer than time  $t$ . As a side note, if we assume that no additional failures happen during the downtime, than this is the same as the instantaneous unavailability  $u(t)$  after an outage, which starts with  $u(0) = 1$  and gives the probability that the system is not yet repaired at time  $t$ . The mean downtime (MDT) is computed by

$$\text{MDT} = \int_0^{\infty} d(t) dt \quad (\text{A.2})$$

Additionally it is known that

$$U = \Lambda \cdot \text{MDT} = \frac{1}{\text{MTBF}} \cdot \text{MDT} \quad (\text{A.3})$$

where  $U$  denotes the steady state unavailability of the system,  $\Lambda$  the failure intensity of the system and MTBF the mean time between failure.

The downtime frequency curve shows how much outages longer than  $t_0$  contribute to the unavailability. In other words, it also computes the unavailability,

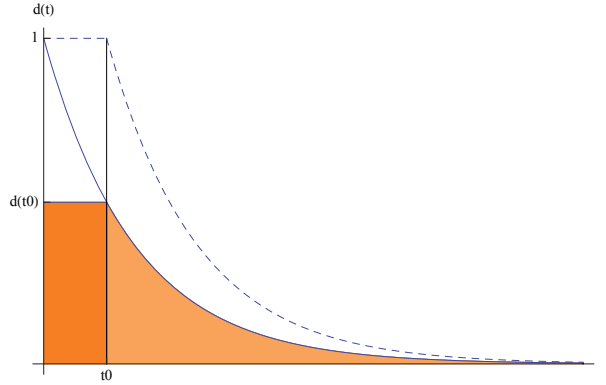


Figure A.1: Calculation of  $MDT_{t_0}$ .

but includes only outages lasting longer than  $t_0$ . In order to compute it, we first compute the  $MDT_{t_0}$ , i.e. the MDT for outages lasting longer than  $t_0$ , and then we compute  $U_{t_0}$ , the unavailability of the system, when only outages lasting longer than  $t_0$  are considered.

As seen in equation A.2 the MDT is computed by integrating  $d(t)$  from 0 to  $\infty$ , i.e. we integrate all downtimes. To compute  $MDT_{t_0}$  we take only those downtimes lasting longer than  $t_0$ . In order to do that, we have to remove the short downtimes and then scale the distribution up, so that the new distribution  $d_{t_0}(t)$  starts with 1, i.e.  $d_{t_0}(0) = 1$ .  $d_{t_0}(t)$  becomes:

$$d_{t_0}(t) = \begin{cases} d(t)/d(t_0) & \text{if } t > t_0 \\ 1 & \text{else} \end{cases}$$

Figure A.1 illustrates the function. The solid line shows  $d(t)$  and the dashed line  $d_{t_0}(t)$ . The colored areas show the unscaled integral of  $d_{t_0}(t)$ . Integrating the function yields:

$$MDT_{t_0} = t_0 + \int_{t_0}^{\infty} \frac{d(t)}{d(t_0)} dt \quad (\text{A.4})$$

If we consider only a subset of all failures, in this case only failures lasting longer than  $t_0$ , then the frequency of failures is lower than when considering all failures. The downtime distribution gives us the probability that failures last longer than  $t_0$  so we can compute the new frequency by

$$\Lambda_{t_0} = \Lambda \cdot d(t_0)$$

And with that we can compute  $U_{t_0}$ , the unavailability of the system, when only outages longer than  $t_0$  are considered:

$$U_{t_0} = \Lambda \cdot d(t_0)(t_0 + \int_{t_0}^{\infty} \frac{d(t)}{d(t_0)} dt) \quad (\text{A.5})$$

## A.2 ENS Frequency Curve

The extension with the energy not supplied (ENS) follows the same reasoning as above. We start with the formula to compute the *mean ENS per outage* which is done by

$$\text{MeanENS} = \int_0^{\infty} e(t) dt$$

and extend it to get the formula for *mean ENS per outages longer than  $t_0$* :

$$\text{MeanENS}_{t_0} = e^*(t_0) + \int_{t_0}^{\infty} \frac{e(t)}{d(t_0)} dt$$

As in equation A.4  $d(t_0)$  is the scaling factor from the downtime distribution.  $e^*(t_0)$  is the energy not supplied up to  $t_0$  caused by only the failures that last longer than  $t_0$ . To calculate it, we need to use the Markov model as explained in the paper, i.e. remove all links from the down states to the up states and compute the accumulated cost until  $t_0$  by

The total ENS costs are then computed by multiplying it with the frequency of these failures as in equation A.5:

$$\text{ENS}_{total}(t_0) = \frac{d(t_0)}{\text{MTBF}} (e^*(t_0) + \int_{t_0}^{\infty} \frac{e(t)}{d(t_0)} dt)$$